DOCUMENT RESUME

ED 441 402	IR 020 434
TITLE	Commission on Child Online Protection (COPA) Report to Congress. Appendices.
PUB DATE	2000-10-20
NOTE	1085p.; For the Commission on Child Online Protection (COPA) Report to Congress, see IR 020 433.
AVAILABLE FROM	For full text: http://www.copacommission.org.
PUB TYPE	Reports - Descriptive (141)
EDRS PRICE	MF08/PC44 Plus Postage.
DESCRIPTORS	Access to Information; *Child Safety; *Children; Federal Legislation; Federal Regulation; Freedom of Speech; *Information Policy; Information Technology; *Internet; Policy Formation; Pornography; Privacy
IDENTIFIERS	Acceptable Use Policy; Commission on Online Child Protection; Filters; First Amendment

ABSTRACT

The appendices for the Commission on Child Online Protection (COPA) Report to Congress, October 20, 2000, include the following: Commission overview, which includes scope and timeline, original statute, amended statute, technologies and methods, and biographies of the commissioners; Commission finances; Commission meetings for the year 2000; materials submitted to the Commission, including materials for hearings as well as research papers, reports, and correspondence; compilation of matrices on filtering, labeling, and rating technologies; Commission responses to questionnaire; and catalog of drawer files, which includes a detailed index of all materials submitted to the Commission in nonelectronic format such as books, software programs, handouts, and VHS tape recordings of hearings and transcripts. (AA)

Reproductions supplied by EDRS are the best that can be made
from the original document.

ED 441 402

Commission on Child Online Protection (COPA)
Report to Congress
October 20, 2000

Appendices

BEST COPY AVAILABLE

IR020434

PERMISSION TO REPRODUCE AND DISSEMINATE THIS MATERIAL HAS BEEN GRANTED BY

K. Litterot

TO THE EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)

1

U.S. DEPARTMENT OF EDUCATION
Office of Educational Research and Improvement
EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)

☐ This document has been reproduced as received from the person or organization originating it.

☐ Minor changes have been made to improve reproduction quality.

- Points of view or opinions stated in this document do not necessarily represent official OERI position or policy.

COPA Commission

Information and Resources About the Commission on Online Child Protection (COPA)

Hosted by the Congressional Internet Caucus Advisory Committee

Appendices to COPA Commission Report

TABLE OF CONTENTS

A. **Commission Overview**

1. Scope and Timeline
2. Original Statute
3. Amended Statute
4. Technologies and Methods
5. Biographies of the Commissioners

B. **Commission Finances**

C. **Commission Meetings**

1. Meeting, March 7, 2000
   Summary
2. Meeting, April 28, 2000
   Agenda
   Minutes
3. Meeting, June 9, 2000
   Agenda
   Minutes
4. Meeting, July 21, 2000
   Minutes (.pdf)
5. Meeting, August 4, 2000
   Minutes (.pdf)
6. Report Drafting Meeting, September 18-19, 2000
   Agenda
   Minutes
7. Report Drafting Meeting, October 4-5, 2000
   Agenda

D. **Materials Submitted to the Commission**
1. Hearing 1, June 8-9, 2000
   Formal Notice
   Guidelines for submitting public comments
   Agenda and Witnesses' Testimony
   Additional Testimony
2. Hearing 2, July 20-21, 2000
   Formal Notice

BEST COPY AVAILABLE

Guidelines for submitting public comments
Agenda and Witnesses' Testimony
Additional Testimony

3. Hearing 3, August 3-4, 2000 Formal Notice
   Guidelines for submitting public comments
   Agenda and Witnesses' Testimony
   Additional Testimony
4. Research Papers and Reports
5. Correspondence (.pdf)

E. **Compilation of Matrices on Filtering, Labeling, and Rating Technologies**

F. **Commission Responses to Questionnaire** (.pdf)

G. **Catalog of Drawer Files**
A detailed index of all materials submitted to the commission in non-electronic format such as books, software programs, and handouts. Also includes VHS tape recordings of hearings and transcripts.

Previous: Conclusion Next: Personal statements of individual Commissioners.

[Home] [Final Report] [About this Site] [FAQ] [The Commission] [Press Room]
[Meetings and Hearings] [Research Papers] [Privacy Policy]

webmaster@copacommission.org / Copyright © 2000

COPA Commission
Information and Resources About the
Commission on Online Child Protection (COPA)
Hosted by the Congressional Internet Caucus Advisory Committee

COPA Commission: Scope & Timeline Proposal

To: COPA Commissioners
From: Don Telage

This memo includes both a discussion proposing the scope of the COPA Commission's inquiry and analysis, and a timeline for producing that analysis.

I. SCOPE

Congress has specifically asked the COPA Commission to conduct a study of six topic areas related to methods for reducing minors' access to material on the Internet that is "harmful to minors." The specific topics the Commission must address are:

A. A common resource for parents to use to help protect minors (such as "one-click-away" resources).
B. Filtering or blocking software or services;
C. Labeling or rating systems;
D. Age verification systems;
E. The establishment of a domain name for posting of any material that is harmful to minors; and
F. Any other existing or proposed technologies or methods for reducing access by minors to such material.

We have also been instructed to analyze each of these types of technology, specifically considering the following:

- Cost of such technologies and methods to parents
- Accessibility of such technologies and methods to parents
- Effect of this technology on law enforcement
- Effect of this technology on privacy
- Effect of this technology on the global and decentralized nature of the Internet

Some of these topics are broader and include a greater number of competitive issues than others. However, in every case, it is necessary that we develop a plan for how to receive and analyze the products, resources, and issues these raise, or we will be overwhelmed by ad hoc requests from those companies and organizations with the resources to do so. A structured approach will be fairer to everyone with an interest in these issues.

II. POSSIBLE APPROACHES

1. Essential Elements

BEST COPY AVAILABLE

There are five specific types of technological resources that the Commission has been instructed to look at, plus "any other" existing or proposed technologies for reducing minors' access to material that is "harmful to minors." The Commission should invite a number of companies to demonstrate their products, making sure that we hear from companies making a range of different products that work in different ways. If we decide to allow any company that wishes to demonstrate a product, we will have to limit the amount of time available to any given product.

Prior to the hearings, the Commission should request information about these products -- how they work, how much they cost, how widely they are used -- from as many companies as possible. In light of proprietary information concerns, I recommend that we make assurances that only aggregate data will be released. (For example, there are X companies that filter using URL lists, there are Y filtered ISPs (perhaps broken down by state), a bar graph reflecting the costs of these products (under $30, $30-50, yearly subscription...) looks like Z.)

Since the best evidence of a product's effectiveness is its track record, the Commission should require that any company whose product is demonstrated submit a list of at least three customers or users, which the Commission may contact for information about the product's effectiveness. Where that product has been submitted for independent or other testing those results should also be obtained. Finally, since the problems encountered by children and families caused Congress to create the Commission, the Commission should solicit, by public notice, written submissions setting out problems, solutions, or their concerns.

Given the robust marketplace of tools in these areas, a minimum of three technology-focused hearings will be necessary.

One hearing on filtering and blocking software and services (item B), including both client-based software and server-based "Filtered ISPs", image recognition, list-based, keyword-based. I would recommend combining this hearing with item C, labeling and rating services, so that the panel can learn about PICS based filtering along with other forms of filtering technology.

A second hearing should cover common resources that are "one-click away" from or available to parents (item A), including, but not limited to: netmom.com; protectkids.com; filtering facts.org; enough.org; childrenspartnership.org; safekids.com; safeteens.com; bluehighways.org; ala.org/parentspage/greatsites and the GetNetWise resource. That hearing should be combined with demonstrations and instruction on age verification technologies (item D) and discussion of establishment of a domain name for posting material that is harmful to minors (item E). While these topics are disparate, each is also narrower in scope than most of the other topics and all three can be covered in one day.

The third hearing and final technology-oriented hearing should focus on item F, other kinds of technological tools and methods. These should include, at a minimum, client-based monitoring software, search engines and subscription services that are oriented towards children, tools that limit the amount of time a given user can spend online, and any other tools that the commission deems important.

2. Given But Resources Enough and Time...
    - Hearings at Varied Locations

      If it is at all possible, all three hearings should be held in different locations. I suggest that we hold one in or near the San Francisco Bay Area/Silicon Valley, one in Austin, Texas, and the third (or more) in Chicago, Virginia (Richmond was suggested at the meeting) or Boston.

    - Commission Academic Studies or Analyses

      Subject to timely availability of funding, a professor or think tank associated with a reputable institution that has not previously taken a position for or against the use of filtering software should be commissioned to study the effectiveness of these tools. They should be specifically instructed to look at a minimum of 2 categories of online material: Does the product filter, block, or specifically note access to a set of unambiguously commercial pornographic Web sites? Does the product filter, block, or specifically note access to a set of Web sites noted as 'misblocked' by such filtering critics as Peacefire or Censorware.org?

      This same study could also analyze and quantify the number of products that indicate they are customizable, and the degree to which that is true; the different categories of information that products filter or say they filter, and the usefulness and accuracy of information provided to a customer about the criteria used to decide whether or not a given site should be filtered.

    - Testimony and Analysis from Experts

      The Commission has specifically been asked to consider the effects that these technologies have on law enforcement, privacy, and the global and decentralized nature of the Internet. Feedback should be sought from law enforcement agencies, privacy advocates, and experts on the global and decentralized nature of the Internet, regarding these topics.

      Subcommittees will be established to gather information from these various sources. Gathering this data will be time-consuming since these sources do not necessarily keep information, which will be of use to the Commission, in a form which is useful. These reports, if gathered on a rolling basis, can add considerably to our ability to question witnesses, consider information from product producers, and consider practical and constitutional limitations.

3. Suggested Timeline

   April 28, 2000 Meeting to finalize scope & plans
   June 8-9, 2000 Hearing on resources that are one-click-away, age verification, and creation of an adult domain.
   July 20-21, 2000 Hearing on filtering & labeling
   August 3-4, 2000 Hearing on other technology
   September 8, 2000 Deadline for expert reports
   October 2, 2000 Draft report circulated to Commission
   October, 2000 Final report circulated to Commission

October 21, 2000 Report submitted to Congress

Also, some time between the first hearing and the expert deadline, we should schedule a consultation and update with the Congressional Internet Caucus.

4. Budget

Supplies	10,000
Phone/Fax	12,000
Postage & Delivery	2,500
Printing	4,000
Books/Subscriptions/Dues	2,500
Office Equipment	2,000
Computer Equipment/Leased	12,000
Travel	5,000
(Meetings & conferences, excluding hearings)	20,000
Furniture & Fixtures	12,000
Network Usage/Web host & design	10,000
Legal & Insurance	25,000
Accounting Fees	3,000
Rent	30,000
Staff	150,000
Secretary/Assistant	50,000
Media	45,000
Chief of Staff (per annum)	120,000
Hearings (3)	240,000
Expert Reports	100,000
Copying & Congressional Outreach	150,000
Total	**1,000,000**

5. Existing Resources

Obviously each of the commissioners, and the companies and organizations they are affiliated with, bring a wealth of knowledge and experience related to our mission. However, as a reference point, there are a number of resources that already exist and should be examined by the commission as we look into these different areas.

A. A Common Resource for Parents

Last summer, the Internet Education Foundation coordinated an industry-wide effort to create a common resource for parents to use to help protect their children, and to put that resource "one-click-away" from parents, wherever they go online. The foundation worked together with experts in children's online safety and content, with nonprofit organizations, and with a broad industry coalition to put together such a comprehensive and ubiquitous resource. It was launched in July 1999 under the name "GetNetWise." GetNetWise includes safety information for children and families, a searchable database of filtering and other technological child-safety tools including over 100 products, a guide to recognizing and reporting trouble online, with links to law enforcement and child advocacy resources, and several collections of Web sites for kids that have been selected by a variety of different experts in this area. In fact, Commissioner Rice Hughes is on the GetNetWise advisory board, and many of the companies serving on this Commission are also sponsors and supporters of GetNetWise.

I invite each of you to look at the GetNetWise central resource, located online at http://www.GetNetWise.org/.

B. Filtering or Blocking Technology

The marketplace for these tools has exploded in parallel to the growth of the Internet. Only a handful of these tools even existed five years ago. In 1998, at the America Links Up kickoff, AT&T Research Labs produced an inventory of available technology. (http://www.research.att.com/projects/tech4kids/) That list included 44 products. In December 1999, the GetNetWise tool database (http://www.GetNetWise.org/tools/) listed over 110 products, and there are many more. Two recent articles, from the New York Times - Cybertimes ("Filtered Internet Services Reach More Religious Groups" October 20, 1999) and from USA Today ("Safe surfing for Web-wary families" August 18, 1999, p. 6D), draw attention to an increasingly popular resource - the filtered Internet Service Provider.

The National Academy of Sciences is in the process of organizing a major study of the effectiveness of filtering and blocking software at protecting children from exposure to obscene sexually explicit material. While our Commission will probably complete our work long before that study is completed, I hope that we will be able to identify a number of resources for the NAS study. Additionally, we should look at the variety of ways these products work, how easy or difficult they are to use, and the degree of decision-making control parents have over what material their children will be able to gain access to when these products are in place. Should we raise the question of schools, libraries, or employers? Both the Freedom to Read Foundation and the National Law Center for Children & Families has written extensive analyses of filtering the Internet in public locations.

On April 13, 2000, the National Coalition for the Protection of Children and Families (independent organization not affiliated with the National Law Center for Children and Families) will be holding a "Tech 2000 Shootout," in Cincinnati, Ohio. This is a daylong event where filtering/blocking technologies will be tested against a single benchmark to allow comparisons to be made. The results of this test should be included in any consideration of technology and a representative of the testing organization allowed to testify or submit written testimony.

C. Labeling and rating systems

This Commission should examine the relationship between rating, labeling and filtering, and consider the differences between third party labeling and rating, and "self-rating" or labeling. This issue has recently been the subject of international attention; the work of the Bertelsmann Foundation, and critics of that work, should be examined by this Commission. We should also question the ease or difficulty of the use of labeling and rating systems, both by parents seeking to make informed decisions about their children's access, and by individuals publishing on the Internet. Under what circumstances will each use such a system? Is voluntary labeling and rating of Web sites meaningful? Are there risks of abuse or government censorship of legal, if controversial, content through the use of mandatory labeling or rating systems?

D. Age Verification Systems

Age verification on the Internet is an issue that the entire industry has been struggling with recently. This Commission should look at the recently released Children's Online Privacy Protection Act (COPPA) rules (http://www.ftc.gov/os/1999/9910/childrensprivacy.pdf), which require Web sites to get parental permission before collecting personally identifiable information from minors under age 13. Many of the statements made to the FTC during this rulemaking process will be informative to this Commission. Additionally, CDT has already released an analysis of the new COPPA rules, identifying what they consider to be the rules' strengths and weaknesses (http://www.ftc.gov/os/1999/9910/childrensprivacy.pdf).

This Commission should also look at commercial age verification systems, such as those currently used by some adult Web sites. (For example, http://www.adultcheck.com/) We should consider their effectiveness - do they really prevent minors from gaining access to material designated for adults? - As well as what burdens they place on adults' access to constitutionally protected speech. Are there age verification systems that allow verified adults, or verified children, to retain privacy or anonymous access to information on the Web? How easy or difficult are they for families to use?

E. Domain Names for Material that is Harmful to Minors

Questions relating to adult-oriented domain names are being addressed in numerous fora, including the federal courts, ICANN, and private industry. This Commission should first gather information from groups that have been considering this question as part of their larger missions.

An idea that is often touted as a way to protect children from inappropriate sexually explicit material is the creation of a new top-level domain with a name like ".xxx". What are the implications of such a domain? Would the owners of adult oriented ".com" sites be required to move to the new domain? Who would decide whether a given Web site must move? Would ".com" adult sites automatically be given the ".xxx" version of a domain name they currently hold? What are the privacy and free expression concerns related to such a domain?

F. Other Technological Options for Protecting Children

There are many technology tools available for parents who are concerned about their children's online experiences. This Commission should request demonstrations of tools in - at least - the following categories:

- Monitoring tools that allow parents to review their children's use of the Internet or the computer;
- Time-limiting tools that allow parents to set the time of day and total amount of time a child can spend online or on the computer;

- Filters that prevent children from giving out personally identifiable information such as their name, address, or telephone number;
- Search engines oriented towards children;
- Closed "green space" Internet based locations designed to give children safe and pre-screened online experiences.

This Commission should gather information on how easy or difficult these kinds of tools are to use, how they work, and what privacy or freedom of speech concerns these types of tools may raise.

The Commission should consider and study how pornography or material harmful to minors is being marketed. Since the Supreme Court considered the Communications Decency Act (CDA), distributors of sexually explicit material have developed and begun using a number of new technologies, which push this material on unsuspecting consumers. The technology being used today must take into account current marketing technologies and strategies as well as identifying how they will address technologies in the future. This is extremely important as the increase in technology convergence quickens. The Commission also should examine currently available and emerging technologies that may help parents counter those marketing efforts.

[Home] [Final Report] [About this Site] [FAQ] [The Commission] [Press Room]
[Meetings and Hearings] [Research Papers] [Privacy Policy]

webmaster@copacommission.org / Copyright © 2000

COPA Commission

Information and Resources About the
Commission on Online Child Protection (COPA)

Hosted by the Congressional Internet Caucus Advisory Committee

Original Statute
TITLE XIV-CHILD ONLINE PROTECTION

SEC. 1401. SHORT TITLE.

This title may be cited as the "Child Online Protection Act".

SEC. 1402. CONGRESSIONAL FINDINGS.

The Congress finds that-

(1) while custody, care, and nurture of the child resides first with the parent, the widespread availability of the Internet presents opportunities for minors to access materials through the World Wide Web in a manner that can frustrate parental supervision or control;

(2) the protection of the physical and psychological well-being of minors by shielding them from materials that are harmful to them is a compelling governmental interest;

(3) to date, while the industry has developed innovative ways to help parents and educators restrict material that is harmful to minors through parental control protections and self-regulation, such efforts have not provided a national solution to the problem of minors accessing harmful material on the World Wide Web;

(4) a prohibition on the distribution of material harmful to minors, combined with legitimate defenses, is currently the most effective and least restrictive means by which to satisfy the compelling government interest; and

(5) notwithstanding the existence of protections that limit the distribution over the World Wide Web of material that is harmful to minors, parents, educators, and industry must continue efforts to find ways to protect children from being exposed to harmful material found on the Internet.

SEC. 1403. REQUIREMENT TO RESTRICT ACCESS BY MINORS TO MATERIALS COMMERCIALLY DISTRIBUTED BY MEANS OF THE WORLD WIDE WEB THAT ARE HARMFUL TO MINORS.

Part I of title II of the Communications Act of 1934 (47 U.S.C. 201 et seq.) is amended by adding at the end the following new section:

"SEC. 231. RESTRICTION OF ACCESS BY MINORS TO MATERIALS COMMERCIALLY DISTRIBUTED BY MEANS OF WORLD WIDE WEB THAT ARE HARMFUL TO MINORS.

"(a) REQUIREMENT TO RESTRICT ACCESS.-
"(1) PROHIBITED CONDUCT.-Whoever knowingly and with knowledge of the character of the material, in interstate or foreign commerce by means of the World Wide Web, makes any communication for commercial purposes that is available to any minor and that includes any material that is harmful to minors shall be fined not more than $50,000, imprisoned not more than 6 months, or both.

"(2) INTENTIONAL VIOLATIONS.-In addition to the penalties under paragraph (1), whoever intentionally violates such paragraph shall be subject to a fine of not more than $50,000 for each violation. For purposes of this paragraph, each day of violation shall constitute a separate violation.

"(3) CIVIL PENALTY.-In addition to the penalties under paragraphs (1) and (2), whoever violates paragraph (1) shall be subject to a civil penalty of not more than $50,000 for each violation. For purposes of this paragraph, each day of violation shall constitute a separate violation.

"(b) INAPPLICABILITY OF CARRIERS AND OTHER SERVICE PROVIDERS.-For purposes of subsection (a), a person shall not be considered to make any communication for commercial purposes to the extent that such person is-

"(1) a telecommunications carrier engaged in the provision of a telecommunications service;

"(2) a person engaged in the business of providing an Internet access service;

"(3) a person engaged in the business of providing an Internet information location tool; or

"(4) similarly engaged in the transmission, storage, retrieval, hosting, formatting, or translation (or any combination thereof) of a communication made by another person, without selection or alteration of the content of the communication, except that such person's deletion of a particular communication or material made by another person in a manner consistent with subsection (c) or section 230 shall not constitute such selection or alteration of the content of the communication.

"(c) AFFIRMATIVE DEFENSE.-

"(1) DEFENSE.-It is an affirmative defense to prosecution under this section that the defendant, in good faith, has restricted access by minors to material that is harmful to minors-

"(A) by requiring use of a credit card, debit account, adult access code, or adult personal identification number;

"(B) by accepting a digital certificate that verifies age; or

"(C) by any other reasonable measures that are feasible under available technology.

"(2) PROTECTION FOR USE OF DEFENSES.-No cause of action may be brought in any court or administrative agency against any person on account of any activity that is not in violation of any law punishable by criminal or civil penalty, and that the person has taken in good faith to implement a defense authorized under this subsection or otherwise to restrict or prevent the transmission of, or access to, a communication specified in this section.

"(d) PRIVACY PROTECTION REQUIREMENTS.-

"(1) DISCLOSURE OF INFORMATION LIMITED.-A person making a communication described in subsection (a)-
"(A) shall not disclose any information collected for the purposes of restricting access to such communications to individuals 17 years of age or older without the prior written or electronic consent of-
"(i) the individual concerned, if the individual is an adult; or

"(ii) the individual's parent or guardian, if the individual is under 17 years of age; and

"(B) shall take such actions as are necessary to prevent unauthorized access to such information by a person other than the person making such communication and the recipient of such communication.

"(2) EXCEPTIONS.-A person making a communication described in subsection (a) may disclose such information if the disclosure is-

"(A) necessary to make the communication or conduct a legitimate business activity related to making the communication; or

"(B) made pursuant to a court order authorizing such disclosure.

"(e) DEFINITIONS.-For purposes of this subsection, the following definitions shall apply:

"(1) BY MEANS OF THE WORLD WIDE WEB.-The term 'by means of the World Wide Web' means by placement of material in a computer server-based file archive so that it is publicly accessible, over the Internet, using hypertext transfer protocol or any successor protocol.

"(2) COMMERCIAL PURPOSES; ENGAGED IN THE BUSINESS.-

"(A) COMMERCIAL PURPOSES.-A person shall be considered to make a communication for commercial purposes only if such person is engaged in the business of making such communications.

"(B) ENGAGED IN THE BUSINESS.-The term 'engaged in the business' means that the person who makes a communication, or offers to make a communication, by means of the World Wide Web, that includes any material that is harmful to minors, devotes time, attention, or labor to such activities, as a regular course of such person's trade or business, with the objective of earning a profit as a result of such activities (although it is not necessary that the person make a profit or that the making or offering to make such communications be the person's sole or principal business or source of income). A person may be considered to be engaged in the business of making, by means of the World Wide Web, communications for commercial purposes that include material that is harmful to minors, only if the person knowingly causes the material that is harmful to minors to be posted on the World Wide Web or knowingly solicits such material to be posted on the World Wide Web.

"(3) INTERNET.-The term 'Internet' means the combination of computer facilities and electromagnetic transmission media, and related equipment and software, comprising the interconnected worldwide network of computer networks that employ the Transmission Control Protocol/ Internet Protocol or any successor protocol to transmit information.

"(4) INTERNET ACCESS SERVICE.-The term 'Internet access service' means a service that enables users to access content, information, electronic mail, or other services offered over the Internet, and may also include access to proprietary content, information, and other services as part of a package of services offered to consumers. Such term does not include telecommunications services.

"(5) INTERNET INFORMATION LOCATION TOOL.-The term 'Internet information location tool' means a service that refers or links users to an online location on the World Wide Web. Such term includes directories, indices, references, pointers, and hypertext links.

"(6) MATERIAL THAT IS HARMFUL TO MINORS.-The term 'material that is harmful to minors' means any communication, picture, image, graphic image file, article, recording, writing, or other matter of any kind that is ob-scene or that-

"(A) the average person, applying contemporary community standards, would find, taking the material as a whole and with respect to minors, is designed to appeal to, or is designed to pander to, the prurient interest;

"(B) depicts, describes, or represents, in a manner patently offensive with respect to minors, an actual or simulated sexual act or sexual contact, an actual or simulated normal or perverted sexual act, or a lewd exhibition of the genitals or post-pubescent female breast; and

"(C) taken as a whole, lacks serious literary, artistic, political, or scientific value for minors.

"(7) MINOR.-The term 'minor' means any person under 17 years of age.".

SEC. 1404. NOTICE REQUIREMENT.

(a) NOTICE.-Section 230 of the Communications Act of 1934 (47 U.S.C. 230) is amended-

(1) in subsection (d)(1), by inserting "or 231" after "section 223";

(2) by redesignating subsections (d) and (e) as subsections (e) and (f), respectively; and

(3) by inserting after subsection (c) the following new subsection:

"(d) OBLIGATIONS OF INTERACTIVE COMPUTER SERVICE.- A provider of interactive computer service shall, at the time of entering an agreement with a customer for the provision of interactive computer service and in a manner deemed appropriate by the provider, notify such customer that parental control protections (such as computer hardware, software, or filtering services) are commercially available that may assist the customer in limiting access to material that is harmful to minors. Such notice shall identify, or provide the customer with access to information identifying, current providers of such protections.".

(b) CONFORMING AMENDMENT.-Section 223(h)(2) of the Communications Act of 1934 (47 U.S.C. 223(h)(2)) is amended by striking "230(e)(2)" and inserting "230(f)(2)".

SEC. 1405. STUDY BY COMMISSION ON ONLINE CHILD PROTECTION.

(a) ESTABLISHMENT.-There is hereby established a temporary Commission to be known as the Commission on Online Child Protection (in this section referred to as the "Commission") for the purpose of conducting a study under this section regarding methods to help reduce access by minors to material that is harmful to minors on the Internet.

(b) MEMBERSHIP.-The Commission shall be composed of 19 members, as follows:

(1) INDUSTRY MEMBERS.-The Commission shall include-

(A) 2 members who are engaged in the business of providing Internet filtering or blocking services or software;

(B) 2 members who are engaged in the business of providing Internet access services;

(C) 2 members who are engaged in the business of providing labeling or ratings services;

(D) 2 members who are engaged in the business of providing Internet portal or search services;

(E) 2 members who are engaged in the business of providing domain name registration services;

(F) 2 members who are academic experts in the field of technology; and

(G) 4 members who are engaged in the business of making content available over the Internet. Of the members of the Commission by reason of each subparagraph of this paragraph, an equal number shall be appointed by the Speaker of the House of Representatives and by the Majority Leader of the Senate.

(2) EX OFFICIO MEMBERS.-The Commission shall include the following officials:

(A) The Assistant Secretary (or the Assistant Secretary's designee).

(B) The Attorney General (or the Attorney General's designee).

(C) The Chairman of the Federal Trade Commission (or the Chairman's designee).

(c) STUDY.-

(1) IN GENERAL.-The Commission shall conduct a study to identify technological or other methods that-

(A) will help reduce access by minors to material that is harmful to minors on the Internet;

and

(B) may meet the requirements for use as affirmative defenses for purposes of section 231(c) of the Communications Act of 1934 (as added by this title). Any methods so identified shall be used as the basis for making legislative recommendations to the Congress under subsection (d)(3).

(2) SPECIFIC METHODS.-In carrying out the study, the Commission shall identify and analyze various technological tools and methods for protecting minors from material that is harmful to minors, which shall include (without limitation)-

(A) a common resource for parents to use to help protect minors (such as a "one-click-away" resource);

(B) filtering or blocking software or services;

(C) labeling or rating systems;

(D) age verification systems;

(E) the establishment of a domain name for posting of any material that is harmful to minors; and

(F) any other existing or proposed technologies or methods for reducing access by minors to such material.

(3) ANALYSIS.-In analyzing technologies and other methods identified pursuant to paragraph (2), the Commission shall examine-

(A) the cost of such technologies and methods;

(B) the effects of such technologies and methods on law enforcement entities;

(C) the effects of such technologies and methods on privacy;

(D) the extent to which material that is harmful to minors is globally distributed and the effect of such technologies and methods on such distribution;

(E) the accessibility of such technologies and methods to parents; and

(F) such other factors and issues as the Commission considers relevant and appropriate.

(d) REPORT.-Not later than 1 year after the enactment of this Act, the Commission shall submit a report to the Congress containing the results of the study under this section, which shall include-

(1) a description of the technologies and methods identified by the study and the results of the analysis of each such technology and method;

(2) the conclusions and recommendations of the Commission regarding each such technology or method;

(3) recommendations for legislative or administrative actions to implement the conclusions of the committee; and

(4) a description of the technologies or methods identified by the study that may meet the requirements for use as affirmative defenses for purposes of section 231(c) of the Communications Act of 1934 (as added by this title).

(e) STAFF AND RESOURCES.-The Assistant Secretary for Communication and Information of the Department of Commerce shall provide to the Commission such staff and resources as the Assistant Secretary determines necessary for the Commission to perform its duty efficiently and in accordance with this section.

(f) TERMINATION.-The Commission shall terminate 30 days after the submission of the report under subsection (d).

(g) INAPPLICABILITY OF FEDERAL ADVISORY COMMITTEE ACT.-The Federal Advisory Committee Act (5 U.S.C. App.) shall not apply to the Commission.

SEC. 1406. EFFECTIVE DATE.

This title and the amendments made by this title shall take effect 30 days after the date of enactment of this Act.

[Home] [Final Report] [About this Site] [FAQ] [The Commission] [Press Room]
[Meetings and Hearings] [Research Papers] [Privacy Policy]

webmaster@copacommission.org / Copyright © 2000

COPA Commission
Information and Resources About the Commission on Online Child Protection (COPA)
Hosted by the Congressional Internet Caucus Advisory Committee

Amended Statute

§ 231. Restriction of access by minors to materials commercially distributed by means of world wide web that are harmful to minors

(a) Requirement to restrict access

(1) Prohibited conduct

Whoever knowingly and with knowledge of the character of the material, in interstate or foreign commerce by means of the World Wide Web, makes any communication for commercial purposes that is available to any minor and that includes any material that is harmful to minors shall be fined not more than $50,000, imprisoned not more than 6 months, or both.

(2) Intentional violations

In addition to the penalties under paragraph (1), whoever intentionally violates such paragraph shall be subject to a fine of not more than $50,000 for each violation. For purposes of this paragraph, each day of violation shall constitute a separate violation.

(3) Civil penalty

In addition to the penalties under paragraphs (1) and (2), whoever violates paragraph (1) shall be subject to a civil penalty of not more than $50,000 for each violation. For purposes of this paragraph, each day of violation shall constitute a separate violation.

(b) Inapplicability of carriers and other service providers

For purposes of subsection (a), a person shall not be considered to make any communication for commercial purposes to the extent that such person is--

(1) a telecommunications carrier engaged in the provision of a telecommunications service;

(2) a person engaged in the business of providing an Internet access service;

(3) a person engaged in the business of providing an Internet information location tool; or

(4) similarly engaged in the transmission, storage, retrieval, hosting, formatting, or translation (or any combination thereof) of a communication made by another person, without selection or alteration of the content of the communication, except that such person's deletion of a particular communication or material made by another person in a manner consistent with subsection (c) or section 230 shall not constitute such selection or alteration of the content of

the communication.

(c) Affirmative defense

(1) Defense

It is an affirmative defense to prosecution under this section that the defendant, in good faith, has restricted access by minors to material that is harmful to minors--

(A) by requiring use of a credit card, debit account, adult access code, or adult personal identification number;

(B) by accepting a digital certificate that verifies age; or

(C) by any other reasonable measures that are feasible under available technology.

(2) Protection for use of defenses

No cause of action may be brought in any court or administrative agency against any person on account of any activity that is not in violation of any law punishable by criminal or civil penalty, and thatthe person has taken in good faith to implement a defense authorized under this subsection or otherwise to restrict or prevent the transmission of, or access to, a communication specified in this section.

(d) Privacy protection requirements

(1) Disclosure of information limited

A person making a communication described in subsection (a)--

(A) shall not disclose any information collected for the purposes of restricting access to such communications to individuals 17 years of age or older without the prior written or electronic consent of--

(i) the individual concerned, if the individual is an adult; or

(ii) the individual's parent or guardian, if the individual is under 17 years of age; and

(B) shall take such actions as are necessary to prevent unauthorized access to such information by a person other than the person making such communication and the recipient of such communication.

(2) Exceptions

A person making a communication described in subsection (a) may disclose such information if the disclosure is--

(A) necessary to make the communication or conduct a legitimate business activity related to making the communication; or

(B) made pursuant to a court order authorizing such disclosure.

(e) Definitions

For purposes of this subsection, the following definitions shall apply:

(1) By means of the world wide web

The term "by means of the World Wide Web" means by placement of material in a computer server-based file archive so that it is publicly accessible, over the Internet, using hypertext transfer protocol or any successor protocol.

(2) Commercial purposes; engaged in the business

(A) Commercial purposes

A person shall be considered to make a communication for commercial purposes only if such person is engaged in the business of making such communications.

(B) Engaged in the business

The term "engaged in the business" means that the person who makes a communication, or offers to make a communication, by means of the World Wide Web, that includes any material that is harmful to minors, devotes time, attention, or labor to such activities, as a regular course of such person's trade or business, with the objective of earning a profit as a result of such activities (although it is not necessary that the person make a profit or that the making or offering to make such communications be the person's sole or principal business or source of income). A person may be considered to be engaged in the business of making, by means of the World Wide Web, communications for commercial purposes that include material that is harmful to minors, only if the person knowingly causes the material that is harmful to minors to be posted on the World Wide Web or knowingly solicits such material to be posted on the World Wide Web.

(3) Internet

The term "Internet" means the combination of computer facilities and electromagnetic transmission media, and related equipment and software, comprising the interconnected world-wide network of computer networks that employ the Transmission Control Protocol/Internet Protocol or any successor protocol to transmit information.

(4) Internet access service

The term "Internet access service" means a service that enables users to access content, information, electronic mail, or other services offered over the Internet, and may also include access to proprietary content, information, and other services as part of a package of services offered to consumers. Such term does not include telecommunications services.

(5) Internet information location tool

The term "Internet information location tool" means a service that refers or links users to an online location on the World Wide Web. Such term includes directories, indices, references, pointers, and hypertext links.

(6) Material that is harmful to minors

The term "material that is harmful to minors" means any communication, picture, image, graphic image file, article, recording, writing, or other matter of any kind that is obscene or that--

(A) the average person, applying contemporary community standards, would find, taking the material as a whole and with respect to minors, is designed to appeal to, or is designed to pander to, the prurient interest;

(B) depicts, describes, or represents, in a manner patently offensive with respect to minors, an actual or simulated sexual act or sexual contact, an actual or simulated normal or perverted sexual act, or a lewd exhibition of the genitals or post-pubescent female breast; and

(C) taken as a whole, lacks serious literary, artistic, political, or scientific value for minors.

(7) Minor

The term "minor" means any person under 17 years of age.

CREDIT(S)
2000 Pocket Part

(Pub.L. 105-277, Div. C, Title XIV, § 1403, Oct. 21, 1998, 112 Stat. 2681-736.)

HISTORICAL AND STATUTORY NOTES

Revision Notes and Legislative Reports

1998 Acts. Statement by President, see 1998 U.S. Code Cong. and Adm. News, p. 582.

Congressional Findings

Pub.L. 105-277, Div. C, Title XIV, § 1402, Oct. 21, 1998, 112 Stat. 2681-736, provided that:

"The Congress finds that--

"(1) while custody, care, and nurture of the child resides first with the parent, the widespread availability of the Internet presents opportunities for minors to access materials through the World Wide Web in a manner that can frustrate parental supervision or control;

"(2) the protection of the physical and psychological well-being of minors by shielding them from materials that are harmful to them is a compelling governmental interest;

"(3) to date, while the industry has developed innovative ways to help parents and educators restrict material that is harmful to minors through parental control protections and self-regulation, such efforts have not provided a national solution to the problem of minors accessing harmful material on the World Wide Web;

"(4) a prohibition on the distribution of material harmful to minors, combined with legitimate defenses, is currently the most effective and least restrictive means by which to satisfy the compelling government interest; and

"(5) notwithstanding the existence of protections that limit the distribution over the World Wide Web of material that is harmful to minors, parents, educators, and industry must continue efforts to find ways to protect children from being exposed to harmful material found on the Internet."

Study by Commission on Online Child Protection

Pub.L. 105-277, Div. C, Title XIV, § 1405, Oct. 21, 1998, 112 Stat. 2681-739, as amended Pub.L. 106-113, Div. B, § 1000(a)(9) [S. 1948, Title V, § 5001(b) to (f)], Nov. 29, 1999, 113 Stat. 1536, 1537-___, provided that:

"(a) Establishment.--There is hereby established a temporary Commission to be known as the Commission on Online Child Protection (in this section referred to as the 'Commission') for the purpose of conducting a study under this section regarding methods to help reduce access by minors to material that is harmful to minors on the Internet.

"(b) Membership.--The Commission shall be composed of 19 members, as follows:

"(1) Industry members.--The Commission shall include 16 members who shall consist of representatives of--

"(A) providers of Internet filtering or blocking services or software;

"(B) Internet access services;

"(C) labeling or ratings services;

"(D) Internet portal or search services;

"(E) domain name registration services;

"(F) academic experts; and

"(G) providers that make content available over the Internet.

"Of the members of the Commission by reason of this paragraph, an equal number shall be appointed by the Speaker of the House of Representatives and by the Majority Leader of the Senate. Members of the Commission appointed on or before October 31, 1999, shall remain members.

"(2) Ex officio members.--The Commission shall include the following officials:

"(A) The Assistant Secretary (or the Assistant Secretary's designee).

"(B) The Attorney General (or the Attorney General's designee).

"(C) The Chairman of the Federal Trade Commission (or the Chairman's designee).

"(3) Prohibition of pay.--Members of the Commission shall not receive any pay by reason of their membership on the Commission.

"(c) First meeting.--The Commission shall hold its first meeting not later than March 31, 2000.

"(d) Chairperson.--The chairperson of the Commission shall be elected by a vote of a majority of the members, which shall take place not later than 30 days after the first meeting of the Commission.

"(e) Study.--

"(1) In general.--The Commission shall conduct a study to identify technological or other methods that--

"(A) will help reduce access by minors to material that is harmful to minors on the Internet; and

"(B) may meet the requirements for use as affirmative defenses for purposes of section 231(c) of the Communications Act of 1934 (as added by this title) [47 U.S.C.A. § 231(c)].

Any methods so identified shall be used as the basis for making legislative recommendations to the Congress under subsection (d)(3).

"(2) Specific methods.--In carrying out the study, the Commission shall identify and analyze various technological tools and methods for protecting minors from material that is harmful to minors, which shall include (without limitation)--

"(A) a common resource for parents to use to help protect minors (such as a 'one-click-away' resource);

"(B) filtering or blocking software or services;

"(C) labeling or rating systems;

"(D) age verification systems;

"(E) the establishment of a domain name for posting of any material that is harmful to minors; and

"(F) any other existing or proposed technologies or methods for reducing access by minors to such material.

"(3) Analysis.--In analyzing technologies and other methods identified pursuant to paragraph (2), the Commission shall examine--

"(A) the cost of such technologies and methods;

"(B) the effects of such technologies and methods on law enforcement entities;

"(C) the effects of such technologies and methods on privacy;

"(D) the extent to which material that is harmful to minors is globally distributed and the effect of such technologies and methods on such distribution;

"(E) the accessibility of such technologies and methods to parents; and

"(F) such other factors and issues as the Commission considers relevant and appropriate.

"(f) Report.--Not later than 2 years after the enactment of this Act [Oct. 21, 1998], the Commission shall submit a report to the Congress containing the results of the study under this section, which shall include--

"(1) a description of the technologies and methods identified by the study and the results of the analysis of each such technology and method;

"(2) the conclusions and recommendations of the Commission regarding each such technology or method;

"(3) recommendations for legislative or administrative actions to implement the conclusions of the committee; and

"(4) a description of the technologies or methods identified by the study that may meet the requirements for use as affirmative defenses for purposes of section 231(c) of the Communications Act of 1934 (as added by this title) [47 U.S.C.A. § 231(c)].

"(g) Rules of the Commission.--

"(1) Quorum.--Nine members of the Commission shall constitute a quorum for conducting the business of the Commission.

"(2) Meetings.--Any meetings held by the Commission shall be duly noticed at least 14 days in advance and shall be open to the public.

"(3) Opportunities to testify.--The Commission shall provide opportunities for representatives of the general public to testify.

"(4) Additional rules.--The Commission may adopt other rules as necessary to carry out this section.

"(l)[sic] Termination.--The Commission shall terminate 30 days after the submission of the report under subsection (d) or November 30, 2000, whichever occurs earlier.

"(m)[sic] Inapplicability of Federal Advisory Committee Act.--The Federal Advisory Committee Act (5 U.S.C. App.) shall not apply to the Commission."

47 U.S.C.A. § 231

47 USCA § 231

[Home] [Final Report] [About this Site] [FAQ] [The Commission] [Press Room]
[Meetings and Hearings] [Research Papers] [Privacy Policy]

webmaster@copacommission.org / Copyright © 2000

COPA Commission

Information and Resources About the
Commission on Online Child Protection (COPA)

Hosted by the Congressional Internet Caucus Advisory Committee

1. Technologies and Methods within the Scope of the COPA Commission

Online information resources (for parents -- e.g., one-click-away)
- Safety information for kids
- Safety information for parents
- Safety information for teenagers
- Educational programs teaching children (or other users) how to conduct targeted searches on the Internet so as to avoid inadvertent exposure to material that may be harmful to minors
- Educational programs teaching law enforcement officers or investigators how to use existing technology to address threats to children that involve the Internet

Filtering software based on a third party provider's negative list
Filtering software based on a third party provider's positive list
Filtering software based on parental decisions to exclude particular sites
Filtering software based on parental decisions to include particular sites
Filtering software based on parental decisions to disapprove specified correspondents
Filtering software based on parental decisions to approve specified correspondents
Filtering software based on labeling/rating adopted by originating site or correspondent
Filtering software based on third party labeling/rating/rules, with parental choice of source of labels/rating/rules sources
Filtering software based on "pixel recognition" decided to block access to only sexually explicit images
Filtering software that is "rules based" meaning filters pages "on the fly" based on mathematical algorithms applied to the content of the page
Filtering software that blocks only the content on a page that has been designated as harmful to minors by the parent/software developer, meaning other text or images on a page may be viewed
Filtering software based on the software developer's negative site list
Filtering software based on the software developer's positive site list
Filtering software that is client (local computer) based
Filtering software that is server (ISP or through other point of access) based
Filtering software that works on the World Wide Web
Filtering software that works on email
Filtering software that works on chat/IRC
Filtering software that works on Instant Message systems
Filtering software that works on usenet news groups
Filtering software that prevents the user from sharing specific personally identifiable information such as last name, address or telephone number
Monitoring software that reports child's online activities to the parent
Monitoring software that otherwise limits extent of child's online activities
Monitoring software that works on the World Wide Web

BEST COPY AVAILABLE

Monitoring software that works on email
Monitoring software that works on chat/IRC
Monitoring software that works on Instant Message systems
Monitoring software that works on usenet news groups
Monitoring software that logs a child's online activities
Parental supervision during Internet usage
Age verification at web site based on credit card
Age verification at web site based on relationship established with a third party site
Age verification at web site based on digital certificates issued to users by certificate authorities
Age verification based on contacting user via email or fax
Age verification through web-of-trust methods
Age verification through biometric technology
Establishment of voluntary domain for sites that self-identify as not suitable for children
Establishment of voluntary domain for sites that self-identify as suitable for children. (e.g. dotKIDS domain)
Establishment of mandatory domain for content meeting some specified standard (e.g. dotXXX domain)
Establishment of a mandatory domain for content intended by the producer to be for adults only
Browser and Site interaction via P3P or similar electronic negotiation protocol to identify and select only sites meeting some specified legal/community standard or subject to specified jurisdiction
Establishment of closed online services aimed at children, with parental involvement in filtering email and approving child's access
Use of the location field of the DNS to specify the geographic location of an originating server
Voluntary use of a password screen/adult verification identifier for adult content sections of a given web site
Mandatory use of a password screen/adult verification identifier for adult content for sites in certain areas
Limiting access by children to Internet connected computers in public places: like schools, libraries and community centers
Providing adults with access to special, screened, computers in libraries and other public places

2. Legal/Policy Questions with respect to each technology and method within the Scope of the COPA Commission

Is the technology or method available now?
Is the technology or method offered by a range of competing companies (in a range of products)?
Is the technology or method easy enough for parents to use?

- Are parents aware of the technology or method?
- If they are not, what barriers are preventing them from becoming aware of it?
- If they are, how has the company or program reached parents?

What is the cost to a web or mail server to implement the technology or method?
What is the cost of the technology or method to end users?

What is the cost imposed by use of the technology or method on other, third parties?
Is the technology or method low enough in cost to encourage parental use?
Is the technology or method low enough in cost to encourage use by noncommercial sites and individuals who publish content?
Can the technology be used by those who publish content on servers that they do not configure or control?
Does the technology or method substantially shield minors from harmful materials?
Does the technology or method render inaccessible substantial amounts of material that is not harmful to minors?
Who determines what material is rendered inaccessible? (The company, the parent, a third partyÉ)
Can a parent review the list of sites that are inaccessible?
If the company or a third party determines what material is rendered inaccessible, are the criteria by which the determination is made available for the parent to review?
Can the parent permanently edit (to make accessible) material that has been rendered inaccessible? Can a parent add to a list of material a site that he or she determines should be inaccessible?
Can a parent temporarily override the decision to render material inaccessible by using a password or other technological means?
When a site or other form of content is rendered inaccessible, is the user alerted to the fact that there is material online that has been rendered inaccessible?
Does the technology or method limit access to images as well as to text? (audio?). Consider separately.
Does the technology or method operate in a predictable and transparent way?
Does the technology or method deal with active messages (incoming email, instant messaging and online chat rooms) as well as web surfing?
Does the technology have any other side effects on the development of Internet standards or on the conduct of other activities on the net?
Would widespread use of this technology or method raise significant first amendment issues?
Would mandatory use of this technology or method raise significant first amendment issues?
Would widespread use of this technology or method impair privacy rights?
Would mandatory use of this technology or method impair privacy rights?
Is this technology or method a less restrictive measure that undermines the constitutional validity of laws imposing more restrictive legal obligations?
Would use of this technology or method have any impact (positive or negative) on legitimate law enforcement?
Would it be feasible to enforce a law requiring use of this technology or method by US based actors?
Would enforcement of a law requiring use of this technology or method by US actors have a substantial impact on availability of harmful materials to minors?
Would enforcement of a law requiring use of this technology or method by US actors have an impact on the distribution or geographic location of sites or mail servers making available material that would violate US law?
May the use of the technology or method by a web site or message originator meet the requirements for use as an affirmative defense by a site/actor that makes material harmful to minors available?
Are further steps needed to make clear that the technology or method provides such an affirmative defense?

[Home] [Final Report] [About this Site] [FAQ] [The Commission] [Press Room]
[Meetings and Hearings] [Research Papers] [Privacy Policy]

webmaster@copacommission.org / Copyright © 2000

COPA Commission

Information and Resources About the Commission on Online Child Protection (COPA)

Hosted by the Congressional Internet Caucus Advisory Committee

THE CHILD ONLINE PROTECTION ACT (COPA) COMMISSION

Commissioners:

- Donald Telage, Network Solutions Inc. - Commission Chairman
- Stephen Balkam, Internet Content Rating Association
- John Bastian, Security Software Systems
- Jerry Berman, Center for Democracy & Technology
- Robert C. Cotner, Evesta.com - resigned
- Arthur H. DeRosier, Jr., Rocky Mountain College
- J. Robert Flores, National Law Center for Children and Families
- Albert F. Ganier III, Education Networks of America
- Michael E. Horowitz, Department of Justice
- Donna Rice Hughes, Author, Kids Online/Founder, Protectkids.com
- William M. Parker, Crosswalk.com
- C. Lee Peeler, Federal Trade Commission
- Gregory L. Rohde, Department of Commerce/NTIA
- C. James Schmidt, San Jose State University
- William L. Schrader, PSINet
- Larry Shapiro, Walt Disney Internet Group
- Srinija Srinivasan, Yahoo! Inc.
- Karen Talbert, Nortel Networks
- George Vradenburg III, America Online, Inc.

[Home] [Final Report] [About this Site] [FAQ] [The Commission] [Press Room]
[Meetings and Hearings] [Research Papers] [Privacy Policy]

webmaster@copacommission.org / Copyright © 2000

BEST COPY AVAILABLE

COPA Commission

Information and Resources About the Commission on Online Child Protection (COPA)
Hosted by the Congressional Internet Caucus Advisory Committee

Donald Telage, Ph.D.
Executive Advisor for Global Internet Strategy
Network Solutions, Inc.

Dr. Telage is currently the Executive Advisor for Global Internet Strategy at Network Solutions, Inc. (NSI). He has been a leading industry strategist on the evolution of the administration and structure of the Internet required for continued commercial growth. He is the senior spokesman for NSI's net strategy, and author of its detailed policy publications on these matters.

From January of 1995 until February, 1997, Dr. Telage was the President and Chief Operating Officer of NSI. Under his leadership, NSI grew into a profitable Internet company, and the world market leader in Registration and Directory services. From 1997 to December of 1999 he was the Senior Vice President of Internet Affairs at NSI. Dr. Telage was a member of the NSI Board of Director from March 1995 to December 1999.

He has held the position of Senior Vice President with Science Applications International Corporation (SAIC), and served on the Board of Directors of the American Registry for Internet Numbers (ARIN) which he helped form in 1997.

Dr. Telage has a Ph.D. and M.A. in Mathematics from Clark University, a Bachelor's Degree in Psychology from the University of Connecticut, and graduate training in Computer Science from the University of Rhode Island.

[Home] [Final Report] [About this Site] [FAQ] [The Commission] [Press Room]
[Meetings and Hearings] [Research Papers] [Privacy Policy]

webmaster@copacommission.org / Copyright © 2000

COPA Commission

Information and Resources About the
Commission on Online Child Protection (COPA)

Hosted by the Congressional Internet Caucus Advisory Committee

Stephen Balkam
Executive Director, Internet Content Rating Association

In a career that stretches back twenty years, Stephen Balkam has demonstrated a capacity for visionary leadership, forward planning, and advocacy at the highest levels of government, business and the non-profit sector. Stephen's remarkable career includes directorships of four organizations, including two start-ups. He has worked with over 100 organizations as a management consultant, trainer and facilitator and is an accomplished public speaker, regularly appearing on television, radio and in the press. He has worked extensively in Europe and the United States and is as much at home with small, local groups as with large, multi-faceted international organizations.

Currently Stephen is the Executive Director of the newly established Internet Content Rating Association and formerly the President of the Recreational Software Advisory Council, an independent, non-profit organization based in Washington, D.C. As the founding President of RSAC and now in his position as Executive Director of IRCA, Stephen has pioneered the development of RSACi - the world's leading content rating system on the Internet. His achievements have been recognized by both the President and Vice President at the first White House Internet Online Summit in July 1996. The RSAC site is regularly featured as one of the Top 100 most popular sites on the web. And in September, RSAC was awarded the prestigious 1998 Carl Bertelsmann Prize for outstanding innovation and responsibility in the Information Society.

During his time with RSAC, Stephen also worked on a consultancy basis as the first Director of the Internet Section of the Software Publishers Association. He coordinated the development and launch of the Electronic Commerce Web Resource - a unique online resource for companies doing business on the Web.

Prior to his appointment with RSAC, Stephen ran his own consultancy business operating in the US and UK, working on issues related to strategic planning, organizational review and restructuring, governance and staff development.

Stephen was the founding Director of the National Stepfamily Association in the UK, the head of the Islington Voluntary Action Council in north London and Director of Camden Community Transport. He worked in the arts at the Institute for Contemporary Arts in central London and was Center Manager at the multi-purpose community arts center, Inter-Action in the early eighties. He also spent time with West Nally - a leading sports sponsorship PR firm and with Burroughs Machines, now Unisys. Stephen has an honors degree (magna cum laude) is Psychology from University College, Cardiff and is the author of *Assessing Your Board's Performance*.

BEST COPY AVAILABLE

[Home] [Final Report] [About this Site] [FAQ] [The Commission] [Press Room]
[Meetings and Hearings] [Research Papers] [Privacy Policy]

webmaster@copacommission.org / Copyright © 2000

COPA Commission
Information and Resources About the
Commission on Online Child Protection (COPA)
Hosted by the Congressional Internet Caucus Advisory Committee

John Bastian
CEO, Security Software Systems, Inc.

Mr. Bastian has been responsible for a wide range of software and hardware development tasks over the past 20 years. Primary functions have included engineering management, software design management and software commercialization activities. Previous software/hardware designs include custom database engines, specialized text gathering resident utilities, speech recognition technology for disabled computer users, specialized text to speech engines and Braille to speech device technology. Current design management of operating system technology that includes new core platforms for monitoring, capturing and analyzing text in any form of from any source. New application designs include Cyber Sentinel child protection software; a content-based monitoring system designed to control sexually explicit Internet traffic by alerting parents to potential problems via e-mail. Newly completed designs include software to perform application, file and directory access control, time management and desktop security for personal computers, and software to reinforce Acceptable Use Policies. Mr. Bastian is married with four children.

Security Software Systems, Inc.
Is a leading edge software developer based in Sugar Grove, Illinois, that specializes in developing security and surveillance applications for consumers, educational facilities, Government, ISPs and Fortune 500 companies. Founded in 1997, the company is successfully developing new technological solutions to security and safety issues related to on-line accessibility. Our product philosophy is to provide highly effective yet flexible solutions to "computer age" problems.

[Home] [Final Report] [About this Site] [FAQ] [The Commission] [Press Room]
[Meetings and Hearings] [Research Papers] [Privacy Policy]

webmaster@copacommission.org / Copyright © 2000

BEST COPY AVAILABLE

COPA Commission
Information and Resources About the Commission on Online Child Protection (COPA)
Hosted by the Congressional Internet Caucus Advisory Committee

Jerry Berman
Executive Director, Center for Democracy & Technology

Jerry Berman is the Executive Director of CDT. The Center was founded in December of 1994 by Mr. Berman and Daniel Weitzner.

Mr. Berman coordinates CDT's free speech and privacy policy working groups comprised of communications firms, associations and civil liberties groups addressing Internet policy issues. He also chairs the Advisory Committee to the Congressional Internet Caucus. Mr. Berman coordinated the successful Citizens Internet Empowerment Coalition challenge to the Communications Decency Act. Mr. Berman has led legislative efforts to enact such landmark legislation as the Electronic Communications Privacy Act of 1986. Prior to founding the Center for Democracy and Technology, Mr. Berman was a Director of the Electronic Frontier Foundation. Mr. Berman was also Chief Legislative Counsel at the ACLU from 1978-1988 and founder and director of ACLU Projects on Privacy and Information Technology.

Mr. Berman received his BA, MA, and LLB at the University of California, Berkeley. He graduated with honors, was elected to Phi Beta Kappa and served as an editor of the California Law Review at Boalt Law School.

[Home] [Final Report] [About this Site] [FAQ] [The Commission] [Press Room]
[Meetings and Hearings] [Research Papers] [Privacy Policy]

webmaster@copacommission.org / Copyright © 2000

BEST COPY AVAILABLE

COPA Commission

Information and Resources About the Commission on Online Child Protection (COPA)

Hosted by the Congressional Internet Caucus Advisory Committee

Robert C. Cotner
President, CEO, Director
Evesta.com

An entrepreneur since his early collegiate days, Mr. Cotner founded and successfully built three construction/real estate companies in the Pacific Northwest over the past 20 years. As a result of those experiences, he learned to excel in dynamic work environments and became highly skilled in project management.

A global thinker and visionary with strong sales and marketing skills, he entered the Internet Service Provider field in 1997. His vision was to provide filtered access to the Internet, protecting users from objectionable material including violence, profanity and pornography. Evesta.com is his fourth business venture.

[Home] [Final Report] [About this Site] [FAQ] [The Commission] [Press Room]
[Meetings and Hearings] [Research Papers] [Privacy Policy]

webmaster@copacommission.org / Copyright © 2000

BEST COPY AVAILABLE

COPA Commission

Information and Resources About the Commission on Online Child Protection (COPA)
Hosted by the Congressional Internet Caucus Advisory Committee

Arthur H. DeRosier, Jr.
President of Rocky Mountain College

Dr. Arthur H. DeRosier, Jr., currently President of Rocky Mountain College, earned his Bachelor of Science degree in history from the University of Southern Mississippi with high honors and his Masters and Doctoral degrees in American history from the University of South Carolina.

He has served as professor of history at The Citadel in Charleston, South Carolina, at Converse College in Spartanburg, South Carolina, and at the University of Oklahoma, East Tennessee State University, where he was appointed as Vice President for Administration, the College of Idaho, and Rocky Mountain College. In addition to his presidency of Rocky Mountain College, he has held the office of the President of East Tennessee State University and the College of Idaho.

He has contributed to the field of education with equal distinction as a scholar and an administrator. His scholarly achievements include the Award of Merit from the American Association for State and Local History for his book, The Removal of the Choctaw Indians, and the "Eagle Feather" Award from The Amerindian, American Indian Review for that same work. The volume Forked Tongues and Broken Treaties, which he co-authored, was selected by the Western Writers of America as the best volume on Western America published in 1975.

Dr. DeRosier has authored and co-authored seven other books, presented twenty scholarly papers, published numerous articles and reviews, and prepared and presented historical educational series for both television and radio. His radio series "An Analysis of the Constitution of the United States" won the George Washington Medallion for educational radio in 1975. He has received an impressive array of fellowship, grants, and awards for his academic achievements.

His attainments as an academic administrator and the state and national consultant are similarly stellar. Dr. DeRosier is presently Chairman of the Independent Colleges of Montana. From 1980-87 he served as a higher education advisor to Idaho's governor John V. Evans, and he acted as an historical consultant for the International Appraisal Company and the U.S. Department of Justice in a federal case dealing with the disposal of Creek Indian lands. He has been a member and chairman of Southern and Northwestern accreditation teams evaluating colleges in the South and West, a member of the board of Editorial Advisors for the Memphis State University Press, was appointed to the NAICU Commission on Tax Policy, and is a member of the Frontier Conference Council of Presidents.

Dr. ReRosier is a member of the Community Advisory Board at Rocky Mountain Bank, and a member of the Billings Rotary Club. He is married to Dr. Linda Scott DeRosier, professor of psychology; he and Dr. DeRosier have four children.

[Home] [Final Report] [About this Site] [FAQ] [The Commission] [Press Room]
[Meetings and Hearings] [Research Papers] [Privacy Policy]

webmaster@copacommission.org / Copyright © 2000

COPA Commission

Information and Resources About the Commission on Online Child Protection (COPA)

Hosted by the Congressional Internet Caucus Advisory Committee

J. Robert Flores

Senior Counsel for the National Law Center for Children and Families

J. Robert Flores is Senior Counsel for the National Law Center for Children and Families. Prior to his arrival at the Law Center, he served as Acting Deputy Chief of the Child Exploitation and Obscenity Section of the Department of Justice, Criminal Division. Mr. Flores was a federal prosecutor with the section for nearly eight years. Prior to his going to the Justice Department he served as an Assistant District Attorney in Manhattan. In that capacity he successfully prosecuted several highly publicized child sexual abuse cases, including a major child prostitution network and a millionaire philanthropist who operated a non-profit organization through which he seduced and sexually abused children.

Bob has prosecuted hundreds of criminal cases in his career. He lectures and teaches regularly at conferences and seminars throughout the United States on criminal procedure, criminal and constitutional law, investigative procedures and computer crime, and has supervised several national investigative programs conducted by the United States Customs Service, United States Postal Service, and the Federal Bureau of Investigation. These projects include the Customs Service's "Operation Long Arm", which targeted individuals in the United States who were importing child pornography from a foreign based bulletin Board Service and "Innocent Images," the FBI's recent effort to address child pornography distribution through America Online, a national Internet service provider. These efforts, by virtue of their innovation and novelty, will make new law in the area of child sexual exploitation and computer crime. Bob has also prosecuted the first federal computer child pornography case, to go to trial, in the matter of U.S. vs. Kimbrough. He successfully argued the appeal to the Fifth Circuit Court of Appeals and the case is now binding precedent for the Circuit.

[Home] [Final Report] [About this Site] [FAQ] [The Commission] [Press Room]
[Meetings and Hearings] [Research Papers] [Privacy Policy]

webmaster@copacommission.org / Copyright © 2000

BEST COPY AVAILABLE

COPA Commission

Information and Resources About the Commission on Online Child Protection (COPA)

Hosted by the Congressional Internet Caucus Advisory Committee

Albert F. Ganier, III
President and CEO
Education Networks of America

Mr. Ganier has served as President and Chief Executive Officer of Education Networks of America (ENA) since founding the company in 1996. He oversaw the initial connection of all 1,800 Tennessee school sites to the Internet, and has managed the network for the past three years. During more than 30 years of business and government experience, he has focused on making technology work for all people - particularly educators and students. In addition to ENA, Mr. Ganier's commitment to improving education starts with his involvement in his three daughter's education and includes student mentoring, school volunteerism, and community leadership.

Mr. Ganier is a successful entrepreneur who previously founded and developed two companies: Trendar Corporation and Milestone Health Services Company. At Trendar, Mr. Ganier helped create a network encompassing over 1,400 locations in 46 states, which communicated with more that 50 different mainframes and was used by 17,000 non-technical employees. His previous experience also includes acting as Executive Vice President (Finance) of American Invesco and its subsidiary, Home Marketing of America. He founded K.G. Equity Resources, an investment-banking firm, and served as Chief of Staff for a U.S. Congressman.

[Home] [Final Report] [About this Site] [FAQ] [The Commission] [Press Room]
[Meetings and Hearings] [Research Papers] [Privacy Policy]

webmaster@copacommission.org / Copyright © 2000

BEST COPY AVAILABLE

COPA Commission

Information and Resources About the
Commission on Online Child Protection (COPA)
Hosted by the Congressional Internet Caucus Advisory Committee

Michael E. Horowitz

Chief of Staff to the Assistant Attorney General for the Criminal Division of the Department of Justice

Michael E. Horowitz currently serves as Chief of Staff to the Assistant Attorney General for the Criminal Division of the Department of Justice. In that position, Mr. Horowitz oversees the Office of Administration and the Office of Policy and Legislation, and provides advice and counsel to the Assistant Attorney General on all legal, policy and administrative issues facing the Criminal Division. Mr. Horowitz also has served as Deputy Assistant Attorney General in the Criminal Division. In that position, Mr. Horowitz supervised the operations of the Child Exploitation and Obscenity Task Section, the Fraud Section and the Campaign Financing Task Force.

Prior to coming to Main Justice, he was an Assistant United States Attorney in the Southern District of New York, having served as Deputy Chief of the Criminal Division and the Chief of the Public Corruption Unit. Mr. Horowitz has received the Attorney General's Distinguished Service Award for his performance in a significant public corruption case, and he has served as an instructor for the Federal Bureau of Investigation, the Justice Department's Office of Legal Education, the United States Department of State, and the New York City Police Department.

[Home] [Final Report] [About this Site] [FAQ] [The Commission] [Press Room]
[Meetings and Hearings] [Research Papers] [Privacy Policy]

webmaster@copacommission.org / Copyright © 2000

BEST COPY AVAILABLE

COPA Commission
Information and Resources About the
Commission on Online Child Protection (COPA)
Hosted by the Congressional Internet Caucus Advisory Committee

Donna Rice Hughes
Author of Kids Online: Protecting Your Children in Cyberspace

Donna Rice Hughes has over 20 years experience in marketing, advertising, communications, public relations and government relations. Mrs. Hughes is the author of Kids Online: Protecting Your Children In Cyberspace. (Revell, September 1998) and has created her own Internet safety website at www.protectkids.com. In 1999, Mrs. Hughes received a Congressional appointment to the Child Online Protection Commission to examine technological solutions to protect children online. She is co-founder and principal of Phoenix Advisory Services which serves small and mid-sized companies in the technology, media and entertainment industries. She is currently working in an advisory role to create and launch FamilyClick.com as the premier safe Internet Service Provider and destination site for the entire family.

From 1994 until July of 1999, Mrs. Hughes served as Communications Director and then Vice President of Enough is Enough, a non-profit educational organization whose mission is make the Internet safe for children and families. Mrs. Hughes led Enough is Enough's efforts regarding the issue of online child safety and played a pioneering role in the national effort to make the Internet safe for children and families. While at Enough is Enough, Mrs. Hughes developed a three-pronged strategy that involves the public, the technology industry and law enforcement sharing the responsibility to protect children on the Internet. This approach has been adopted by many industry and government leaders.

She is frequently sought out by the media, policy makers, law enforcement officials and industry leaders for her expertise on solutions for ensuring that children have a safe and rewarding experience online. Donna has given over 1700 media interviews and has been a featured guest on numerous television shows including *CNN's Crossfire, Dateline, The Today Show, Oprah* and *The View*. Additionally, her views on the issue have been featured in publications including *The Wall Street Journal, The New York Times, The Los Angeles Times, USA Today, The San Francisco Chronicle, The San Jose Mercury News* and *McCalls Magazine*. She has spoken extensively on the subject in educational and professional forums across the country including Johns Hopkins University, MIT, American University, The Freedom Forum, The National Press Club and testified before Congress on the issue of Internet dangers and safety following the Columbine tragedy.

Mrs. Hughes served on the steering committee for the Internet Online Summit: Focus on Children in December of 1997 and served on the executive committee for the Summit's public awareness campaign, America Links Up. She currently serves on the advisory board for the Get Net Wise industry initiative.

Mrs. Hughes received a Bachelor of Science Degree from the University of South Carolina and graduated Magna Cum Laude and Phi Beta Kappa.

[Home] [Final Report] [About this Site] [FAQ] [The Commission] [Press Room]
[Meetings and Hearings] [Research Papers] [Privacy Policy]

webmaster@copacommission.org / Copyright © 2000

COPA Commission

Information and Resources About the
Commission on Online Child Protection (COPA)

Hosted by the Congressional Internet Caucus Advisory Committee

William M. Parker
President and Chief Executive Officer
crosswalk.com

In April 1998 Mr. Parker began directing the management of crosswalk.com (NASDAQ:AMEN). Mr. Parker led the re-branding of the Web presence as crosswalk.com, the redesign of the site to make it the Christian community portal or home base, and the retooling of the technology into a database driven Internet publishing environment. Mr. Parker directed the launch of multiple unique channels for the very large niche of Christian conservatives, including a comprehensive, values-based personal finance channel which provides exclusive information on over 9000 mutual funds. This lets values-conscious investors know if their mutual fund is profiting from investments in companies involved with pornography, abortion, and/or antifamily entertainment. Mr. Parker has placed an emphasis on Christian music, making the crosswalk.com Christian Music Channel the number one rated Christian Music Site for '98 by combining unique content with the opportunity to listen to 6 Web radio stations, click and listen to tracks of the most recent Christian music, and the opportunity to purchase online. As a service to the community, in November '98 crosswalk.com became the first Web presence to offer both Internet filtering and safe search free from the site. With this, and channels addressing Careers, Spiritual Life, Entertainment, Men, Women, and News, all supported by a national marketing campaign, Mr. Parker has positioned crosswalk.com to be the preferred, comprehensive, and invigorating host to Christians on the Web. Mr. Parker recently appeared on CNBC on two separate occasions to discuss crosswalk.com's approach to values based investing, Internet safety, and overall Internet business building. In addition, the company has received recent coverage from Money Magazine, Business Week, CBS Market Watch, and feature articles by the *Washington Post* and the *Washington Times*.

Prior to coming to crosswalk.com, Mr. Parker was Executive Vice President and Manager of CACI's Integrated Information Systems Division, leading in the development information systems, Year 2000 conversion, business process re-engineering, internet-based electronic commerce, automated procurement, and simulation. CACI is a public information technology company, with annual revenues exceeding $300 million. Mr. Parker's business represented about one quarter of the company's revenues.

Previously, Mr. Parker, as Director of Business Development, attracted over $775 million in new business and played a key role in a corporate turn around from five years of flat performance to sustained growth. In this position he directed business and technology planning, marketing, sales, proposal development, and played a key role in corporate acquisitions. From 1982 until 1992 Mr. Parker developed an information systems and systems engineering business from initiation to sustaining over $25 million in annual revenues.

A graduate of the U.S. Naval Academy in '76 and Navy officer until '82, he led in engineering and tactical roles aboard ship, and in teaching ROTC at the University of South Carolina.

Mr. Parker lives in Philomont, Virginia, with his wife of 23 years, Linda McCrone Parker.

[Home] [Final Report] [About this Site] [FAQ] [The Commission] [Press Room]
[Meetings and Hearings] [Research Papers] [Privacy Policy]

webmaster@copacommission.org / Copyright © 2000

COPA Commission
Information and Resources About the Commission on Online Child Protection (COPA)
Hosted by the Congressional Internet Caucus Advisory Committee

C. Lee Peeler

Associate Director, Division of Advertising Practices, Federal Trade Commission

C. Lee Peeler, Esq., has directed the Federal Trade Commission's Division of Advertising Practices since 1985. The Division is responsible for development of agency policy with regard to national advertising. It has prepared guidance and prosecuted cases involving advertising for foods, OTC drugs, dietary supplements, alcohol, and tobacco. The Division also has played a critical role in development of Internet advertising policy.

Mr. Peeler joined the FTC as a staff attorney in 1973. During his career, he has held a number of management positions in the Bureau of Consumer Protection and has spoken and lectured widely on issues of truth in advertising.

Mr. Peeler received his B.A. and J.D. degrees from Georgetown University.

[Home] [Final Report] [About this Site] [FAQ] [The Commission] [Press Room]
[Meetings and Hearings] [Research Papers] [Privacy Policy]

webmaster@copacommission.org / Copyright © 2000

BEST COPY AVAILABLE

Gregory L. Rohde

Assistant Secretary of Commerce for Communications and Information, Administrator of the National Telecommunications and Information Administration

On August 3, 1999, President Clinton nominated Gregory L. Rohde to serve as the Assistant Secretary of Commerce for Communications and Information. He was confirmed by the United States Senate on November 10, 1999. The Assistant Secretary is responsible for formulating policies supporting the development and growth of telecommunications, information and related industries; furthering the efficient development and use of telecommunications and informational services; providing policy and management for federal use of the electromagnetic spectrum; and providing telecommunications facilities grants to public users.

Mr. Rohde served as a senior aide to U.S. Senator Byron L. Dorgan (D-ND) for more than ten years as the chief policy advisor for all areas of jurisdiction under the Senate Committee on Commerce, Science, and Transportation, of which Senator Dorgan is a member, including telecommunications and technology issues. He played a key role in many important legislative initiatives such as the landmark *Telecommunications Act of 1996* (which provided for a comprehensive reform of all aspects of the telecommunications and media industries) and the *Internet Tax Freedom Act of 1998* (which provided a moratorium on state and local taxation on electronic commerce).

He began his career as a legislative assistant to then-Representative Byran L. Dorgan in 1988, serving as chief policy advisor for health care, social security, and human resource issues on the House Committee on Ways and Means, of which Representative Dorgan was a member. Additional legislative areas of responsibility included education, judiciary, environment, and transportation. Prior to joining then-Representative Byron L. Dorgan, Mr. Rohde was an instructor teaching social justice classes at Mackin Catholic High School in Washington, D.C.

Mr. Rohde also served as a Team Coordinator for the Health Care Financing Administration Section in the Health and Human Services Cluster of the Presidential Transition Team for the Clinton-Gore Administration and as Campaign Manager for the Nicholas Spaeth for Governor Campaign (D-ND) in 1992.

Born in Pierre, South Dakota in 1961, Mr. Rohde's family moved to North Dakota when he was young, settling in the state capitol of Bismarck where he graduated from Century High School in 1980. He was a state champion distance runner, setting state records in the mile and two-mile and received All-American honors in track.

Mr. Rohde attended Colorado University in Boulder, Colorado and North Dakota State University in Fargo, North Dakota, on a track and cross-country scholarship. He received a Bachelor of Science in Education with majors in Philosophy and Sociology from North

BEST COPY AVAILABLE

Dakota State University in 1985 and a Bachelor of Sacred Theology from the Catholic University of America, Washington, D.C., in 1988.

[Home] [Final Report] [About this Site] [FAQ] [The Commission] [Press Room]
[Meetings and Hearings] [Research Papers] [Privacy Policy]

webmaster@copacommission.org / Copyright © 2000

COPA Commission

Information and Resources About the Commission on Online Child Protection (COPA)

Hosted by the Congressional Internet Caucus Advisory Committee

C. James Schmidt

Professor, San Jose State University

James Schmidt has been a university librarian and professor for over 35 years. Currently, Schmidt serves as a Professor at San Jose State University. He has held posts at Brown University, Ohio State University and has consulted with university and state library systems all across the country.

Since coming to San Jose State, Schmidt has served as the University's first Chief Information Officer. In this role, he works on an ongoing basis with a number of Silicon Valley companies on the development and implementation of the University's telecommunications infrastructure.

Schmidt has served on a number of state and federal committees on information technology including the California State University Commission on Learning Resources and Instructional Technology, California State University Council of Library Directors, the Networking Task Force for the State Library of California and the Network Advisory Committee on the Library of Congress. He has also served as an active member of a number of professional associations including the American Library Association, the Center for Research Libraries and the Association of Research Libraries.

Schmidt holds a bachelor's degree from Catholic University, a master's degree from Columbia University and a Ph.D. from Florida State University. He has also done graduate study work in Political Science at the University of Texas and Ohio State University.

[Home] [Final Report] [About this Site] [FAQ] [The Commission] [Press Room]
[Meetings and Hearings] [Research Papers] [Privacy Policy]

webmaster@copacommission.org / Copyright © 2000

BEST COPY AVAILABLE

COPA Commission

Information and Resources About the
Commission on Online Child Protection (COPA)
Hosted by the Congressional Internet Caucus Advisory Committee

William L. Schrader
Chairman and Chief Executive Officer
PSINet

William L. Schrader is chairman of the board of directors, chief executive officer, and founder of PSINet, one of the world's largest and most experienced commercial Internet service providers. Publicly traded on the NASDAQ market as PSIX, PSINet operates in 22 countries, serves over 80,000 companies, and offers a broad suite of advanced Internet, Web and eCommerce products.

Schrader has authored numerous position statements, spoken at industry events, and appeared on Capitol Hill to present industry and corporate positions on such issues as Internet encryption, the domain name system, and the Communications Decency Act. In addition, he has participated in panel discussions of industry trends and issues on mainstream media such as CNBC, MSNBC, CNNfn, First Business, and TechnoPolitics.

As PSINet chairman and CEO, Schrader has been instrumental in the formation of industry groups such as the Commercial Internet Exchange (CIX). He is also the driving force behind PSINet's innovative global peering initiative for Internet service providers worldwide. Schrader was named 1998 Master Entrepreneur of the Year by Ernst & Young and he was listed as one of the industry's "20 to Watch" by Computer Reseller Magazine and "Top 10 to Watch" by Telephony Magazine.

Prior to forming PSINet in 1989, Schrader was founder, president, and chief executive officer of NYSERNet, a corporation that created the first regional Internet network, providing networking services to university, corporate, and government communities in New York state. Earlier, Mr. Schrader was executive director and co-founder of two supercomputer centers, one at Cornell University and one at Syracuse University. While at Cornell, he led the development of the NSFNET Backbone Network to connect the national supercomputer centers, which became the basis for the NSFNET system.

Mr. Schrader earned a bachelor of science degree in biology from Cornell University, as well as completing graduate work in business and finance.

[Home] [Final Report] [About this Site] [FAQ] [The Commission] [Press Room]
[Meetings and Hearings] [Research Papers] [Privacy Policy]

webmaster@copacommission.org / Copyright © 2000

BEST COPY AVAILABLE

COPA Commission

Information and Resources About the Commission on Online Child Protection (COPA)

Hosted by the Congressional Internet Caucus Advisory Committee

Larry Shapiro

Executive Vice President, Corporate Development and General Counsel Walt Disney Internet Group

As general counsel and executive vice president at GO.com, Larry Shapiro serves as the company's general counsel and also oversees human resources and public affairs. A key player in the formation of GO.com, Larry previously served as executive vice president, business development and operations for Disney's online unit, Buena Vista Internet Group (BVIG).

Prior to the November 1999 merger of Infoseek Corporation and BVIG, Larry was BVIG's chief liaison with Infoseek for several key GO Network areas: business and legal affairs, product development and marketing. Before that, Larry was senior vice president, business and legal affairs for BVIG, where he served as general counsel.

Prior to joining BVIG, Larry was vice president-counsel within Disney's corporate legal department, where he led numerous transactions including Disney's acquisition of Starwave and its 1998 investment in Infoseek.

Before joining Disney, Larry was an associate at two Los Angeles-area law firms: Weil, Gotshal & Manges, and O'Melveny & Myers. He earned his undergraduate degree from the University of Pennsylvania and his JD from the University of Michigan.

Larry and his wife live in Encino, California with their dog, Greta.

[Home] [Final Report] [About this Site] [FAQ] [The Commission] [Press Room]
[Meetings and Hearings] [Research Papers] [Privacy Policy]

webmaster@copacommission.org / Copyright © 2000

BEST COPY AVAILABLE

Srinija Srinivasan

Vice President, Editor-in-Chief, Yahoo! Inc.

Srinija Srinivasan is the driving force behind Yahoo!'s team of human editors and is responsible for the development of original content throughout Yahoo!'s global network of properties. In particular, Srinivasan directs the designs and maintenance of Yahoo!'s overall classification and organization scheme, making it the most intuitive, robust, expandable, and efficient guide for online information and discovery. Srinivasan has extensive educational and practical experience in information organization and artificial intelligence. Prior to joining Yahoo! as the company's fifth employee, Srinivasan was involved with the Cyc Project, a ten-year artificial intelligence effort to build an immense database of human commonsense knowledge, via two companies: Microelectronics and Computer Technology Corporation (MCC) and Cycorp. At Cycorp, Srinivasan independently managed the company's California-based office, and helped develop the Cyc technology into innovative areas such as database browsing and integration.

Srinivasan holds a B.S. with distinction from Stanford University in Symbolic Systems and conducted course work in Japan. She is proficient in both written and spoken Japanese. Other professional and academic accomplishments include a summer intensive in Japan as a researcher and programmer for Fujitsu Laboratories, and published research papers in highly-acclaimed journals including *Government Information Quarterly* and the *Journal of Technology Transfer*. Srinivasan has appeared in top publications both locally and nationally, including *The New York Times* and *Fortune*, was named one of "The Net 50" by *Newsweek*, and was selected as one of the "40 Under 40" by *San Francisco Focus* for their second-annual brain trust.

[Home] [Final Report] [About this Site] [FAQ] [The Commission] [Press Room]
[Meetings and Hearings] [Research Papers] [Privacy Policy]

webmaster@copacommission.org / Copyright © 2000

BEST COPY AVAILABLE

COPA Commission

Information and Resources About the Commission on Online Child Protection (COPA)

Created by the Congressional Internet Caucus Advisory Committee

Karen Talbert
Director of Performance Consulting
Nortel Networks

Karen Talbert joined Nortel Networks in April 2000 as Director of Performance Consulting for the Sales Development Organization. She is consulting with Nortel Major Accounts, which sell telecommunications and network solutions. Her role is to facilitate account development and unified strategies by working with the Executive Sales Leadership and Account Teams.

Previously Karen was Director of Product Marketing with AmeriVision where she was responsible for marketing strategies and the introduction of new products and services. Her work led to the development and launch of ifriendly.com, the filtered Internet access offered by AmeriVision, which provides "family friendly" Internet services.

Karen has over 20 years experience in the telecommunications industry, including expertise in data communications and computing sales and service. Her experience includes all aspects of sales, project, sales and marketing management and operational service management.

[Home] [Final Report] [About this Site] [FAQ] [The Commission] [Press Room]
[Meetings and Hearings] [Research Papers] [Privacy Policy]

webmaster@copacommission.org / Copyright © 2000

BEST COPY AVAILABLE

COPA Commission

Information and Resources About the Commission on Online Child Protection (COPA)

Hosted by the Congressional Internet Caucus Advisory Committee

George Vradenburg III

Senior Vice President for Global and Strategic Policy
America Online, Inc.

George Vradenburg is America Online, Inc.'s (AOL) Senior Vice President for Global and Strategic Policy. A member of the office of the Chairman, Mr. Vradenburg sets the company's strategic course on evolving policy issues facing the interactive medium.

Mr. Vradenburg joined AOL as General Counsel in early 1997, and, in under two years, has become a key voice in the online industry, helping to shape the interactive policy debate in the United States and overseas. Mr. Vradenburg's mission - in working with governments and industry leaders locally, nationally and around the world - is to help craft a policy framework that will guide the online medium into the next millennium in a way that promotes the public interest, as the Internet reshapes business and society.

The array of policy issues on which Mr. Vradenburg has helped AOL lead the industry include: protecting consumer privacy online, winning industry support for a pledge of "zero tolerance" for crimes against children online, campaigning against junk e-mail (spam), protecting intellectual property online and developing a new framework for e-commerce and international trade.

He is a frequent speaker in this country and overseas on Internet policy. He has testified before Congress on electronic commerce, copyright and privacy issues, and was a featured speaker at the 1997 Bonn Ministerial Conference on electronic commerce. Mr. Vradenburg serves on the boards of the Lawyers' Committee for Human Rights, the Internet Policy Institute, the Internet Content Rating Association (Europe), and the Northern Virginia Technology Council. He is a member of the UCLA Center for Communication Policy's Board of Governors and a Visiting Scholar of the Annenberg School of Communications, University of Southern California.

Mr. Vradenburg previously served as Senior Vice President and General Counsel of CBS, Inc. and as Executive Vice President of Fox, Inc. Prior to joining America Online, he was a senior partner in the Los Angeles office of Latham & Watkins and co-chair of its Entertainment & Media Practice Group. He received his B.A. from Oberlin College and his J.D. from Harvard Law School in 1967.

[Home] [Final Report] [About this Site] [FAQ] [The Commission] [Press Room]
[Meetings and Hearings] [Research Papers] [Privacy Policy]

webmaster@copacommission.org / Copyright © 2000

BEST COPY AVAILABLE

COPA Commission

Information and Resources About the Commission on Online Child Protection (COPA)

Hosted by the Congressional Internet Caucus Advisory Committee

Report on Commission Finances:

The Commission on Child Online Protection did not receive any funding from Congress and relied upon gifts and grants from the private sector. The Commission received gift and grant authority from Congress on June 30, 2000. Below is a copy of the language as it appeared in Title IV of the E-Sign bill.

TITLE IV-COMMISSION ON ONLINE CHILD PROTECTION

SEC. 401 AUTHORITY TO ACCEPT GIFTS.

Section 1405 of the Child Online Protection Act (47 U.S.C. 231 note) is amended by inserting after subsection (g) the following new subsection:

'(h) GIFTS, BEQUESTS, AND DEVISES-The Commission may accept, use, and dispose of gifts, bequests, or devises of services of property, both real (including the use of office space) and personal, for the purpose of aiding or facilitating the work of the Commission. Gifts or grants not used at this termination of the Commission shall be returned to the donor or grantee.'

Gifts and Grants:

The Commission's operations were made possible by contributions of time by numerous individuals and companies, and by $70,000 in monetary grants from Network Solutions Inc.; Yahoo! Inc.; America Online, Inc.; Education Networks of America; and PSINet Inc. These contributions of time and funds were supplied unconditionally and with no expectation or receipt of consideration in any form from the Commission, under statutory gifts and grants authority.

This funding paid for direct costs and professional fees on behalf of the COPA Commission.

The following is an account of expenditures by the COPA Commission from July 1, 2000-September 30, 2000:

COPA Financial Information (7/1 -- 9/30/00)

BEST COPY AVAILABLE

Office Administration: (Facsimile, Photocopy, Postage)	$7,820.91
Media kits (Collating and distribution)	$288.98
Deliveries (Overnight and messenger)	$692.24
Travel:	$1198.86
Press Release Distribution:	$1,268.31
Transcripts:	$2,808.16
Supplies:	$19,868.03
Witness expenses:	$10,424.63
Meals:	$3,474.87
Telephone and Conference call charges:	$2,029.20
AV costs:	$3,790.00
Room and equipment rental:	$1,994.07
Letterhead design, production and printing:	$742.61
Media Monitoring/Broadcast Schedule:	$103.27
News Research/Back issues:	$82.11
TOTAL	**$38,686.25**
Payment for remaining direct costs plus professional fees for Dittus Communications:	$31,313.75
TOTAL:	**$70,000.00**

The following is an account of the additional donations made to the Commission:

- Lunch for Commission in Richmond 7/21 $266 (America Online Inc.)
- Hearing 3 Room Rental/Equipment 8/4 $680 (San Jose State University)
- Hearing 3 A/V Rental 8/4 $945 (Yahoo! Inc.)
- Hearing 3 Thursday lunch, 8/3 $1021.43 (U.S. Postal Service)
- Hearing 3 food 8/3-8/4 $515 (San Jose State University)
- September meeting A/V costs 9/18-9/19 $1,600 (Department of Justice)

In-kind Contributions:

- Congressional Internet Caucus Advisory Committee--web site design and hosting.
- America Online Inc.-meeting room space, AV costs and food for October meeting.

Once the Commission's report is delivered to Congress, Rocky Mountain College in Billings, Montana will review and provide a letter of assurance about the Commission's finances.

[Home] [Final Report] [About this Site] [FAQ] [The Commission] [Press Room]
[Meetings and Hearings] [Research Papers] [Privacy Policy]

webmaster@copacommission.org / Copyright © 2000

COPA Commission

Information and Resources About the
Commission on Online Child Protection (COPA)
Hosted by the Congressional Internet Caucus Advisory Committee

COPA COMMISSION MEETING

March 7, 2000

Location: Department of Commerce/NTIA

Don Telage of Network Solutions was appointed Chairman of the COPA Commission.

[Home] [Final Report] [About this Site] [FAQ] [The Commission] [Press Room]
[Meetings and Hearings] [Research Papers] [Privacy Policy]

webmaster@copacommission.org / Copyright © 2000

BEST COPY AVAILABLE

COPA Commission

Information and Resources About the Commission on Online Child Protection (COPA)

Hosted by the Congressional Internet Caucus Advisory Committee

AGENDA FOR THE CHILD ONLINE PROTECTION ACT (COPA) COMMISSION MEETING

April 28, 2000

Date and Time:

Friday, April 28--9:00 a.m. to 4:00 p.m.

Location:

Federal Trade Commission
600 Pennsylvania Avenue, N.W.
Room 332
Washington, D.C.
(use the Pennsylvania Avenue entrance closest to 6th Street)

Parking is limited so we suggest that attendees take cabs. When you arrive at the FTC, you must go through the metal detector, show identification, sign in, and receive a badge. Then proceed to the elevator to the 3rd floor.

Agenda:

9:00 a.m. Welcome remarks and charge to the Commission by Don Telage, chairman of the COPA Commission

9:15 a.m.-11:00 p.m. Review agenda for the meeting
Update on funding for the COPA Commission
Review work plan:
    Scope proposal: Technologies and Evaluation Criteria
    Subcommittees: Structure membership and leadership

11:00 a.m.-11:15 a.m. Break

11:15 a.m.-12:30 p.m. Discussion and decision on hearing schedule, topics, location and format
Schedule of future Commission meetings

12:30 p.m.-2:00 p.m. Break for lunch **(lunch on your own)**

2:00 p.m.-4:00 p.m. Panel Discussion and Q&A with experts on the Communication Decency Act (CDA) and Child Online Protection Act (COPA) legislation and litigation:

David Crane, Senate Commerce Committee
John Morris, Jenner and Block
Bruce Taylor, National Law Center for Children and Families
Chris Hansen, ACLU

4:00 p.m. Adjourn

[Home] [Final Report] [About this Site] [FAQ] [The Commission] [Press Room]
[Meetings and Hearings] [Research Papers] [Privacy Policy]

webmaster@copacommission.org / Copyright © 2000

COPA Commission

Information and Resources About the
Commission on Online Child Protection (COPA)
Hosted by the Congressional Internet Caucus Advisory Committee

Minutes of the Child Online Protection Act (COPA) Commission meeting

Friday, April 28, 2000
Federal Trade Commission (Room 332)
9:00 a.m. to 4:00 p.m.

The following commissioners were present:

- Donald Telage, Network Solutions Inc. - Commission Chairman
- Stephen Balkam, Internet Content Rating Association
- John Bastian, Security Software Systems
- Jerry Berman, Center for Democracy & Technology
- Arthur H. DeRosier, Jr., Rocky Mountain College
- J. Robert Flores, National Law Center for Children and Families
- Albert F. Ganier III, Education Networks of America
- Michael E. Horowitz, Department of Justice
- Donna Rice Hughes, Author, Kids Online/Founder, Protectkids.com
- C. Lee Peeler, Federal Trade Commission
- William M. Parker, Crosswalk.com
- Gregory L. Rohde, Department of Commerce/NTIA
- C. James Schmidt, San Jose State University
- Karen Talbert, Nortel Networks

Larry Shapiro, Walt Disney Internet Group, participated by conference call.

Elizabeth Frazee served as a proxy for George Vradenburg, AOL; John Scheibel served as a proxy for Srinija Srinivasan, Yahoo! Inc.; and John LoGalbo served as a proxy for William L. Schrader, PSINet. Robert Cotner with Evesta.com was called away and could not attend the meeting.

9:00 a.m. to 12:30 p.m.

Don Telage, chairman of the Commission, welcomed the COPA Commissioners and asked for any additions to the meeting agenda. No additions were made.

Chairman Telage noted that the Commission's role is to lay out the range of technologies and methods that could be used to help reduce access by minors to "harmful to minors" material. Telage stated that a key task of the Commission will be to define the criteria that should be used in evaluating these technologies and methods.

Chairman Telage then gave an update on the funding situation for the Commission. He reported that the Commission has no funding, no sponsoring body or governmental secretariat, and no ethics officer. Chairman Telage has been told by congressional staff that the Commission has wide bipartisan support and that it should receive funding. Funding is, however, unlikely before mid-July and is dependent on the passage of an appropriate Supplemental Appropriations measure.

Commissioner William Parker recommended that the Commission contact House Speaker Hastert's office and have a designated staffer attend meetings. Commissioner Jerry Berman said that the Commission should be considered under the jurisdiction of Congress.

Commissioner Berman recommended sending a letter to the Commerce committee chairman and ranking members in both the House of Representatives and the Senate stating that the Commission is under the assumption that the Commission is under the jurisdiction of Congress and that Congress should clarify the Commission's status.

Chairman Telage noted that his understanding was that the legislative change eliminating funding and sponsorship was accidental, and that there was a significant possibility that the Commission would be funded.

Commissioner Bob Flores gave an update on the Largent amendment that was attached to the House Supplemental Appropriations bill. The amendment would provide $750,000 in funding for the COPA Commission. The bill passed the House, but there is no such amendment in the Senate at this time. Commissioner Flores said that another option would be to have the agencies of the ex officio Commissioners obtain funding for the Commission in anticipation of a Congressional appropriation.

Commissioner Rohde stated that the legislative change to "unfunded" was not, to his understanding, accidental, and suggested that the Commission go back to Congress with requests for funding.

The COPA Commission voted to send two letters to the House and Senate leadership as well as to Commerce Committee chairman and ranking members. The first letter will focus on Congress taking responsibility for the Commission. The second letter will outline the funding dilemma. Commissioners Berman and Flores will draft the letters and forward them to Chairman Telage for review. Chairman Telage will sign the letters on behalf of the Commissioners. A subset of the Commission will then arrange a meeting with leadership and members of the Commerce Committee. Commissioner Flores will head the subcommittee to meet with staff. Representatives designated by Commissioners Vradenburg and Srinivasan will join him.

Commissioner Al Ganier reported that Senate Majority Leader Lott is ready to have a meeting on the funding issue. Sen. Lott's chief of staff has told Commissioner Ganier that the error in funding was not deliberate. Commissioner Ganier will set up a meeting between Senator Lott, Don Telage and ENA's Vice President for Government Relations.

Chairman Telage reported that until the Commission receives funding, Commissioners can line up private support to help them personally, but not the Commission.

Chairman Telage said that there would be no guarantee of reimbursement for those that assist Commissioners. He noted that the Tax Advisory Commission had had an express statutory provision allowing gifts and grants, but that the COPA Commission had no such authority. He also noted that the Commission needed an authoritative source of ethics advice to assist with these questions.

Discussion of Scope and Timeline Document included in briefing book:

The Commission has until October 21, 2000 to submit a report to Congress. The Commission may have to ask for an extension, but Chairman Telage said the Commission should work toward that deadline. He said that the Commission will create subcommittees to plan each of the three hearings and that the subcommittees should work in parallel on each hearing. The hearings would be scheduled for 1.5 days each, to be followed by a half-day Commission meeting.

Commissioner Balkam asked what the format of the hearings would be. Chairman Telage said he envisions experts testifying on balanced panels. There will be an open microphone to allow public comments at the conclusion of the hearing.

Commissioner Rohde added that the Commission should make hearing transcripts available on a web site and allow people to make comments over the Internet.

Commissioner Flores said that the Commission should talk to the Congressional Internet Caucus about posting COPA Commission content on the caucus's website.

It was decided that each planning subcommittee will develop an outline for the scope of the hearing and that the plan will then be reviewed by the entire Commission. Elizabeth Frazee emphasized that the planning subcommittees must be balanced.

Commissioner Karen Talbert said that the Commission should have a baseline understanding of "what is filtering." She said the Commission should develop guidelines and a scope and definition document for the various technologies. Commissioner Talbert also mentioned testing companies' financial plans.

Commissioner Donna Rice Hughes said that the Commission must set standards for products and test the claims of companies. Chairman Telage responded, saying that the goal is to discuss possible and existing technologies rather than particular products.

Discussion of a suggested timeline for hearings:

The Commission voted to tentatively schedule the following hearings:

June 8 and 9 - Resources that are one-click-away, age verification and creation of an adult domain.
July 20 and 21 - Filtering and labeling
August 3 and 4 - To be determined (other technologies)

Discussion of the report format:

Chairman Telage recommended that the Commission report be short and not too technical so that it is useful to Congress (perhaps 20-30 pages). The point was made that the appendix must include all appropriate information underlying the Commission's evaluations. It was recommended that a good record of the hearing be kept and that all of the public comments be included in the report.

Commissioner Flores said that the testimony must be reported and transcribed, and recommended that the ex officio members be responsible for recordkeeping for the hearings. He also recommended having exhibits at the hearings.

There was a discussion about who should keep all correspondence, papers and files for the Commission. It was decided that Kristin Litterst would keep files and a log of all information and phone calls. Commission members should send materials intended for the entire Commission to Litterst and Telage.

Commissioner DeRosier asked if the second hearing should build on the first hearing. Chairman Telage said that the hearings should be considered independently.

Discussion of subcommittees:

Commissioners Flores and Berman volunteered to serve as co-chairs for the subcommittee arranging the first hearing on resources that are one-click away; age verification and creation of an adult domain.

The following commissioners expressed interest in participating in the subcommittee on the filtering and labeling hearing: Commissioners Vradenburg, Schmidt, Rice Hughes, Parker and Balkam. Elizabeth Frazee, sitting in for Commissioner Vradenburg, agreed that Commissioner Vradenburg would to convene a conference call of the subcommittee participants and report this information back to Chairman Telage.

The following Commissioners volunteered to serve on the subcommittee planning the third hearing: Commissioners Bastian, Vradenburg, Berman, Srinivasan, Flores, Ganier and Schrader. Commissioner Bastian will convene a conference call and report back to Chairman Telage.

Rice Hughes asked the Chairman to consider assigning more than two co-chairs that have different philosophical points of view to the subcommittees. Commissioner Ganier said that one person could serve as the chairman of the subcommittee and one would serve as executive director.

The Commission voted to have Chairman Telage decide who should serve as co-chairs for the second and third hearings. Chairman Telage said he would take all comments into consideration and notify the Commission on Monday, May 1 of his decision by email.

Discussion of the Technologies and Methods document:

Chairman Telage introduced a matrix as a guide for evaluating each technology and method.

Commissioner Berman noted that "methods" (such as acceptable use policies and consumer education) should be added to the document.

Commissioner Flores recommended assigning technical experts in the various agencies so the Commission can query them. Flores asked whether the hearings were for merely looking at technology or also for analyzing the legal impact of a given technology. Telage responded that the matrix should be used to question witnesses at the hearing.

Commissioner Rohde stated that as the plan for each hearing is prepared, the plan should be circulated among the commissioners. The ex officio members would then take the material and give it to the proper people within their agencies to review and make suggestions (i.e., with respect to adding witnesses). The agencies would follow the same procedure when the report is being drafted.

Chairman Telage noted that it is the responsibility of the Commission to choose a venue and to make decisions about how they want to set up each hearing.

Charges to the Commission:

1. Make editorial comments on the Scope and Timeline document. Send changes to Chairman Telage and Kristin Litterst by COB Friday, May 5.
2. Review the technologies and methods document and make changes. This document will serve as the framing matrix for guiding the committee. Send changes to Chairman Telage and Kristin Litterst by COB Friday, May 5.

Both documents will be revised and distributed to the Commission the week of May 8.

The co-chairs planning the first hearing will draft a scope and plan by COB May 5. The draft will be distributed by Kristin Litterst to the Commission. The deadline for a similar document for the other two hearings is May 12.

Alan Davidson said that any Commissioner that has expertise on resources that are one-click away, age verification, and top level domains should contact him.

Commissioner Lee Peeler asked if the Commission will consider push technologies - how the industry markets their products - at the first hearing. These technologies could be considered at both the first and third hearings.

Commissioner DeRosier commented that he is concerned that the elimination of funding from COPA was not inadvertent. He wants to make sure that Congress pays attention to the Commission and realizes all the work and expertise that is going into this report. He said the report deserves a congressional hearing at the end.

Commissioner Berman said that passing the statute was the focus of Congress. The Commission was an add-on made without much deliberation by Congress.

Chairman Telage said that the Commission must maintain a positive outlook. He reiterated that the central goal of the Commission is to reach a constructive conclusion.

Break for lunch 12:30 p.m. -2:00 p.m.

2:00 p.m.-4:00 p.m.

The afternoon session of the Commission meeting featured a panel discussion about the Communications Decency Act and the Child Online Protection Act legislation and litigation.

The purpose of the panel was to further educate Commissioners about the history of these issues in Congress, the legislation, and the resulting litigation. The Commissioners need an understanding of these issues in order to be able to address the challenging questions that will come before the Commission during the hearing process.

Panelists:

David Crane is a professional staff member for the Senate Committee on Commerce, Science and Transportation, working for Sen. John McCain. Before coming to work for Chairman McCain, Crane served as legislative director for Sen. Dan Coats where he assisted in drafting the final Senate version of the CDA, managed the bill through final Congressional passage, and coordinated preparation of the Congressional brief in support of the CDA. In addition, Crane prepared the Senate version of COPA, managed it through final passage, and coordinated preparation of the Congressional brief in support of the COPA.

David Crane discussed the evolution of CDA and COPA legislation in Congress.

John B. Morris, Jr. is a partner in the Washington, D.C. office of Jenner & Block, where he practices in trial and appellate courts in the fields of the Internet, telecommunications, and First Amendment law. Mr. Morris was a lead counsel on behalf of the American Library Association, America Online, Microsoft, and other association and industry plaintiffs in the ACLU v. Reno/American Library Association v. U.S. Dep't of Justice challenge that overturned the Communications Decency Act. In that case, Mr. Morris had primary responsibility for the written and testimonial presentation of evidence about Internet technology to the courts. More recently, Mr. Morris was actively involved in an amicus curiae effort supporting the challenge to COPA.

John Morris gave an overview of the litigation surrounding both the CDA and COPA.

Bruce Taylor is the President and Chief Counsel of the National Law Center for Children and Families. He was most recently a Senior Trial Attorney for the Child Exploitation and Obscenity Section of the U.S. Department of Justice. Mr. Taylor first served as a Prosecutor and Assistant Director of Law for the City of Cleveland, prosecuting several hundred obscenity cases and appeals, including an argument before the United States Supreme Court. For ten years, Mr. Taylor was then General Counsel to Citizens for Decency through Law, Inc., where he assisted prosecutors, police, and legislators nationwide in the enforcement, investigation, and improvement of laws against obscenity, child pornography and exploitation, and child sexual abuse. He also served as Assistant Attorney General of Arizona. Since 1973, he has prosecuted nearly 100 state and federal obscenity jury cases, as well as trials on prostitution, RICO, child pornography, and child sexual abuse, has written over 200 appeal and amicus curiae briefs, presented over 50 appellate arguments, and has represented public officials and law enforcement personnel in civil lawsuits on civil rights, zoning, nuisance abatement, injunction and forfeiture actions, criminal procedure, and federal challenges to federal, state, and municipal laws.

Bruce Taylor discussed the litigation and the definition of "harmful to minors."

Chris Hansen has been affiliated with the ACLU as an attorney since 1973, when he joined the staff of the ACLU-sponsored Mental Health Law Project. Since 1984, Mr. Hansen has worked as an attorney with the national ACLU, where he holds the position of senior staff counsel. In that capacity, he was lead counsel in Reno v. ACLU, the ACLU's historic and successful challenge to federal Internet content regulations. He is also lead counsel in the first -- and equally successful -- challenges to state censorship statutes in Georgia (ACLU v. Miller) and New York (ALA v. Pataki). In the New York case, the court found that states cannot regulate the Internet.

Chris Hansen discussed four principles that were considered during the CDA litigation.

After the panel concluded, the Commissioners asked questions. The meeting concluded at 4:30 p.m.

[Home] [Final Report] [About this Site] [FAQ] [The Commission] [Press Room]
[Meetings and Hearings] [Research Papers] [Privacy Policy]

webmaster@copacommission.org / Copyright © 2000

COPA Commission

Information and Resources About the Commission on Online Child Protection (COPA)

Hosted by the Congressional Internet Caucus Advisory Committee

Agenda of the Commission on Online Child Protection (COPA) meeting

The Commission on Child Online Protection (COPA) Meeting
June 9, 2000

Date and Time:

Friday, June 9, 2:00p.m.- 4:30p.m.

Location:

Federal Trade Commission
600 Pennsylvania Avenue, N.W.
Room 432
Washington, D.C.
(use the Pennsylvania Avenue entrance closest to 6th Street)

Parking is limited so we suggest that attendees take cabs. When you arrive at the FTC, you must go through the metal detector, show identification, sign in, and receive a badge. Then proceed to the elevator to the 4th floor.

Agenda:

2:00p.m.-2:15p.m.

Opening remarks from Don Telage, Chairman, COPA Commission. Commissioners review and adjust meeting agenda.

2:15 p.m.-2:45p.m.

Chair update on funding for the COPA Commission. Establish subcommittee to deal with funding and budget.

2:45p.m.-3:15p.m.

Discuss and critique Hearing #1.

3:15p.m.-3:30p.m.

Break

BEST COPY AVAILABLE

3:30p.m.- 4:15p.m.

Oral report from Subcommittee Chairpersons of Hearing #2. Oral report from Subcommittee Chairpersons of Hearing #3. Discuss hearing schedule, topics, location and format. Approve final Scope and Timeline document. Approve final Technologies and Methods matrix.

4:15p.m.- 4:30p.m.

Establish Commission report drafting subcommittee. Added agenda items (if any).

4:30p.m.

Adjourn

[Home] [Final Report] [About this Site] [FAQ] [The Commission] [Press Room]
[Meetings and Hearings] [Research Papers] [Privacy Policy]

webmaster@copacommission.org / Copyright © 2000

COPA Commission
Information and Resources About the Commission on Online Child Protection (COPA)
Hosted by the Congressional Internet Caucus Advisory Committee

Minutes of the Commission on Online Child Protection (COPA) meeting

Friday, June 9, 2000
Federal Trade Commission (Room 432)
2:00 p.m. to 4:00 p.m.

The following commissioners were present:

- Donald Telage, Network Solutions Inc. - Commission Chairman
- Stephen Balkam, Internet Content Rating Association
- John Bastian, Security Software Systems
- J. Robert Flores, National Law Center for Children and Families
- Donna Rice Hughes, Author, Kids Online/Founder, Protectkids.com
- C. Lee Peeler, Federal Trade Commission
- William M. Parker, Crosswalk.com
- C. James Schmidt, San Jose State University
- Karen Talbert, Nortel Networks
- George Vradenburg, AOL

Proxies sat is for the following commissioners: Alan Davidson for Jerry Berman, Center for Democracy & Technology; Kathy Rodi for Albert F. Ganier III, Education Networks of America; Hemanshu Nigam for Michael E. Horowitz, Department of Justice; and Sallianne Fortunato for Gregory L. Rohde, Department of Commerce/NTIA.

2:00 p.m. to 4:00 p.m.

Don Telage, chairman of the Commission, welcomed the COPA Commissioners and asked for any additions to the meeting agenda. The following items were added to the agenda: media relations and extension of the Commission.

Update on Funding:

Chairman Telage then gave an update on the funding situation for the Commission. He reported that gift and grant language was added to the E-Signature bill that is now being considered in the conference committee. Chairman Telage has been told by congressional staff that the conference report may be approved as early as the week of June 12. Once the gift and grant authority is approved, Telage suggested that the Commission consider creating guidelines for accepting private funding. He reported that he has met with the staff for the Internet Tax Commission and was told that the Commission accepted dollars from a few of the Commission members and once Congress funded the Commission, those members were repaid. Telage also reported that the Largent Amendment, which would give $750,000 to the Commission, was approved as part of the Supplemental Appropriations measure. An amendment which would give the Commission $1.5 million in funding and designate the Department of Commerce as the sponsoring agency is moving through the Senate as part of the Supplemental Agriculture bill. Commissioner Bob Flores stated that he is worried about the gift and grant authority language because many of these large companies are contacted over and over again about giving money to Commissions and it puts non-profit organizations at a disadvantage.

Commissioner Vradenburg asked how much money the Commission really needs?

Chairman Telage responded that the Commission has not been able to do a number of things because of the lack of funding. He cited transcription of hearings and meetings; witness travel; commissioner travel; and buying expert reports as examples.

Commissioner Vradenburg stated that it doesn't sound like that would equal more than $100,000.

Chairman Telage responded that it's closer to $500,000 and above.

Commissioner Vradenburg said that the Commission still needs funding from Congress. He said even if The Commission receives congressional funding, that does not mean that those that contribute money through the gift and grants authority will be repaid. He commented that the Internet Tax Commission members were limited to contributing $50,000 each.

Commissioner Flores said that any offers to provide funding to the Commission must be communicated immediately to the Commission. He discussed setting up a subcommittee to set guidelines for accepting funding.

Commissioner Vradenburg emphasized not spending a lot of money. He suggested using personal staff to help the Commission.

Chairman Telage pointed out that not everyone has personal staff to use.

Alan Davidson sitting in for Commission Berman recommended setting up a subcommittee to come up with criteria for receiving funding.

Chairman Telage established a subcommittee on funding. Members of the subcommittee are: Commissioners Schmidt, Berman, Flores and Chairman Telage. The subcommittee will come up with recommendations on how to accept funding by COB on June 16.

Commissioner Flores commented that the Visa witness didn't seem to want to share numbers. He said that the Commission needs to push to get real data on market and economic issues.

Hemanshu Nigam sitting in for Commissioner Horowitz suggested that the Commission separate the company from the data, and create a survey to elicit responses.

Chairman Telage discussed a need for having an independent third party research some of the data the Commission is seeking.

Commissioner Rice Hughes commented that the Commission needs a validation mechanism for this data.

Discussion and Critique Hearing #1

Commissioner Balkam recommended that there be more diversity at the next hearings. He also said that we should make more of an effort to invite people we don't know to testify.

Alan Davidson for Commissioner Berman added that the Commission needs to hear real life stories from people who can talk about their experiences.

Commissioner Rice Hughes commented that there was overkill with regard to the panel of "one-click-away" resources. She recommended that the Commission devote more time to understanding various technologies. Commissioner Rice Hughes said more time should be given to dig deeper and get recommendations from witnesses. She suggested considering a fourth hearing. Commissioner Rice Hughes added that we only had one legal perspective on the panel regarding age verification. We need to balance that perspective.

Commissioner Schmidt said that it is crucial that whoever is communicating with potential witnesses give them a sharply honed focus on what they are supposed to cover in their testimony.

Chairman Telage agreed and added that the witnesses did not answer the questions that were provided to them by the Commission before they testified.

Commissioner Parker said the Commission needs to admit if we don't have time to do this well.

Chairman Telage then moved up the discussion regarding extending the commission.

Extending the Commission:

Alan Davidson for Commissioner Berman said that the new Congress will want to see the results of the Commission. He recommended not extending past March.

Commissioner Vradenburg said he does not see a need for an extension. He suggested possibly deferring the third hearing and reminded Commissioners that that the Commission does not have the power to extend our life.

Chairman Telage noted that he is concerned about writing this report based on testimony he heard at the first hearing. He said we did not get the quality of questioning we needed.

Commissioner Vradenburg pointed out that we are in the process of digestion after the first hearing.

Chairman Telage noted that the Commission does not have to make the decision now about whether to ask Congress for an extension.

Commissioner Flores pointed out that between now and the next hearing we will know the appropriations situation in Congress. He cautioned putting off this discussion too long and having the decision made for us.

Liza Kessler for Commissioner Vradenburg asked the Commission to weigh in more on witness selection and other topics during the planning process for the next two hearings.

Oral report from Subcommittee Chairpersons on Hearing #2

Commissioner Rice Hughes reported that the hearing 2 subcommittee has the following three working groups:

1. Logistics
2. Matrix on Filtering, Labeling and Rating
3. Witnesses

Commissioner Rice Hughes noted that the second hearing will be held in Richmond, Virginia. Chairman Telage explained that Rep. Bliley had offered a university in Richmond as a venue for the second hearing. He said that a meeting with Rep. Bliley's staff will be scheduled for the week of June 12.

Commissioner Rice Hughes reported that a draft matrix had been e-mailed to the Commission the previous week. The draft matrix also was handed out at the meeting. Commissioner Rice Hughes said the subcommittee needs suggestions from the Commission on the rating and labeling portion of the matrix. The deadline to provide comments to the subcommittee is Tuesday, June 13.

Commissioner Rice Hughes announced that the next conference call to discuss witnesses for the second hearing is June 13. Sallianne Fortunato for Commissioner Greg Rohde reported the dates of the next three conference calls: June 20, July 5 and July 18.

Alan Davidson for Commissioner Berman recommended that the subcommittee circulate the draft witness list earlier to the Commission to allow more input from Commissioners.

Janet Evans for Commissioner Lee Peeler recommended that the subcommittee change the metrix and give witnesses multiple choice answers instead of asking open-ended questions. She said the Commission would receive more responses.

Commissioner Vradenburg reported that the first draft of the witness list and agenda will completed by the Tuesday, June 13 conference call. He encouraged input from other Commissioners. Commissioner Vradenburg suggested having children testify before the Commission on how to avoid adult sites.

Liza Kessler for Commissioner Vradenburg noted that the Commission should hear from tech witnesses more than vendors because Commissioners need to understand the technology. She suggested setting up a technology demonstration over lunch for those who do not testify. Kessler said that would be a way for these different companies to get their information into the record. She cautioned that trying to decide who to invite to testify will be a challenge.

Commissioner Talbert suggested having two computers side-by-side, displaying examples of filtered vs. non-filtered products.

Commissioner Rice Hughes emphasized that the Commission must find a way to evaluate the technologies.

Chairman Telage recommended hiring an independent third party to evaluate the different technologies.

Alan Davidson for Commissioner Berman recommended locating people who can analyze the market.

Commissioner Vradenburg noted that the Commissioner needs to know to what extent is the product being used in the marketplace. He said we need to find out if users use the technology and are they satisfied. He recommended getting teenagers to test products.

Commissioner Flores commented that the Commission could face an attack or defamation suit if we are evaluating technologies.

Commissioner Vradenburg agreed saying the Commission must be careful in how we describe the shortcomings of various technologies. He said AOL would be reticent to discuss competitors but would discuss parental controls broadly.

Commissioner Talbert agreed that children are a good test of products. She recommended having an anonymous panel of children to test products and breaking the filtering section into two categories: software based filters and server-based filters.

Commissioner Balkam noted that the Commission must clarify who the users are. He said parents buy the products and the children are affected based on the parents decision.

Commissioner Talbert emphasized that filter-based products are reluctant to disclose their subscriber base.

Commissioner Schmidt said there is a definite distinction between software filtering devices and server filtering devices--some target the server and others target the ISP.

Commissioner Vradenburg recommended giving an overview regarding the range of products and their usersÑproducts that are currently in use and those coming down the pike. He asked the Commission to think of people who could give such an overview at the next hearing.

Chairman Telage emphasized that the Commission should not be discussing specific products.

Commissioner Vradenburg said the role of the Commission is to be educators not product promoters.

Oral Report from Subcommittee Chairpersons on Hearing #3:

Commissioner Balkam reported that focus will be a challenge for the third hearing. He emphasized that time is short. He listed the categories that he envisions being covered by the third hearing.

Focus: Other kinds of existing or proposed technology tools and methods To include: client-based monitoring software; children orientated search engines; subscription services orientated towards children; time limiting tools; personal information filters; "green space" or "child safe space"; email, chat and "whisper" mode monitoring; acceptable use policies New and proposed technologies: wireless; push technology; broadband; convergence; ubiquitous/always on access.

Kathy Rodi for Commissioner Ganier announced that there will be a conference call for the third hearing on June 21 at 11 a.m. EST.

Commissioner Balkam reported that the subcommittee is planning to hold the third hearing in San Jose or another California location. He recommended holding a technology demonstration at this hearing as well.

Commissioner Bastian asked if the third hearing has to address issues that were not wrapped up in the first two hearings.

Chairman Telage answered no. He said these first three hearings might be a first round, an orientation and acclamation on the issues because the Commissioners aren't experts on all these technologies and we don't have the resources or time. Chairman Telage said that an extension of the Commission might make sense.

Commissioner Rice Hughes seconded extending the Commission. She recommended holding a fourth hearing to dip deeper into the issues and technologies. She said that the Commission has a great opportunity and a challenge to come up with a report of real value for our kids and the future of the Internet.

Commissioner Vradenburg said the Commission needs a clearer work plan to get from here to the final report that is due November 30. He recommended moving the third hearing into September. Commissioner Vradenburg noted that the first and second hearing are more informational, but that the Commission must dig deeper in the third hearing.

Alan Davidson for Chairman Berman said that hearing 3 will be more than a catchall for the other two hearings. He recommended that issues such as greenspaces etcÉ must be covered.

Approval of final Scope and Timeline/Technologies and Methods Documents

The Commission voted to put the Scope and Timeline document and the Technologies and Methods document on the COPA Commission web site with the caveat that these documents are subject to change.

Establish Commission Report Drafting Subcommittee:

Chairman Telage recommended creating a subcommittee to draft guidelines to writing the report to Congress. He emphasized that the report should stand alone and support the recommendations of the Commission. Chairman Telage issued a charge to the subcommittee to: 1) draft an annotated outline and 2) develop a methodology that balances quality and efficiency. The Commission will use this methodology to deal with different sections of the report.

Subcommittee members will be: Commissioners Vradenburg, Berman, Schmidt, Flores, Rohde and Chairman Telage. The subcommittee to provide initial recommendations by COB Friday, June 30.

Commissioner Rice Hughes requested that other Commissioners be able to provide input.

Discussion of Media Relations

Commissioner Balkam discussed the need to communicate to Capitol Hill and the public about the potential impact of the Commission's work. He suggested proactive media relations and the development of a question and answer document.

Commissioner Schmidt reported that he has had calls from the press and in each case he refers reporters to Chairman Telage who speaks for the Commission.

Commissioner Flores said he speaks to the press as to what his role is and what he expects from the Commission, but that he understands Chairman Telage speaks for the Commission.

Chairman Telage agreed saying that the Commissioners should be able to speak as Commissioners but not on behalf of the Commission. It was decided that the Commissioners would review the current question and answer document and send comments to Kristin Litterst.

Commissioner Rice Hughes recommended that all Commissioners use their individual public relations opportunities to talk about the importance of the Commission.

Kristin Litterst for Chairman Don Telage asked the Commissioners to distribute any media materials, including hearing advisories, to their press lists.

The meeting concluded at 4:00 p.m.

---

webmaster@copacommission.org / Copyright © 2000

Commission on Child Online Protection
Meeting Minutes
July 21, 2000

Present: Commissioners Telage (chair), Rice Hughes, Vradenburg, Berman, Parker, Horowitz, Ganier, Flores, Bastian, Balkam, Schmidt and Talbert.

Janet Evans sat in for Commissioner Peeler and Kelly Levy sat in for Commissioner Rohde.

Meeting began at 1:30 p.m.

Chairman Telage began the meeting by noting the topics the Commission planned to discuss: (1) the state of the Commission's private and public funding; (2) the status of plans for Hearing 3; and (3) the Commission's report.

Funding

1. Private funding

Chairman Telage reported that he has received pledges of funding from AOL ($10,000), Commissioner Ganier ($10,000), and PSINet ($10,000). Network Solutions (now part of Verisign) has contributed $30,000, for a total of $130,000 spent on staff to the chair and other direct Commission costs. The NSI money will pay for Kristin Litterst's services through August 4 only, and $10,000 of the other pledged funds has been committed for witness travel for the third hearing (August 3-4, 2000).

Chairman Telage said that he planned to speak to Commissioner DeRosier later on July 21, and that he would ask DeRosier to be the fiscal agent for the Commission. Commissioner DeRosier has also volunteered to lead the Commission's effort to raise privacy funds on the condition that others volunteer to help.

Commissioners Berman and Vradenburg volunteered to assist with private fundraising.

2. Public funding

Commissioner Telage reported that an agriculture supplemental bill was in conference, but that it is very uncertain whether that bill will include funding for the Commission. Commissioners Berman, Flores, and Rice Hughes have volunteered to come up with an action plan for forwarding the progress of legislation funding the Commission.

Commissioner Telage noted that it is obvious that the Commission will require additional funding after August 4, when the NSI money and other pledged funds run out.

Commissioner Vradenburg asked how much money the Commission needed to get through the end of November 2000. Kristin Litterst and Chairman Telage responded that the amount was probably less than $250,000. Chairman Telage has prepared a budget covering this period. Commissioner Vradenburg noted that it would be useful to tell funding sources that that was the level of support that was needed. Chairman Telage noted that the scope of the Commission's budget depends in part on the intensity of interaction planned by the Commission in connection with its report.

Hearing 3

Commissioner Balkam reported that planning for Hearing 3 was in better shape than it had been, but that there was still much to be done. He noted that there will be a strong panel on other technologies and methods for this hearing, but that the globalization panel has only the equivalent of half a person on it, and the new technology panel has only the equivalent of two and a half people on it (out of twelve the planning subcommittee for Hearing 3 has considered). Commissioner Balkam noted that non-industry people needed travel support to be witnesses at Hearing 3. There will be a conference call to further plan Hearing 3 at 11 a.m. on Monday, July 24.

Commissioner Schmidt reported that the Hyatt St. Clair (spelling uncertain) is the closest hotel to Hearing 3. Attendees will be unable to drive through the campus, and the hearing room is a two-block walk from any parking structure. The hearing room is 50% larger than the University of Richmond hearing room was. The Commission will be the guest of the School of Library Science at the University of San Jose. Yahoo! has agreed to pay for telecommunications/computer links needed for Hearing 3.

Chairman Telage asked whether there would be an opportunity for another dinner in San Jose for the Commissioners and staff. Kristin Litterst said that she would work on arranging this.

Commissioner Telage asked that Commissioners assist in locating and contacting witnesses for Hearing 3. Commissioner Balkam noted that vacation schedules and the Republican convention were making it difficult to obtain witnesses.

Report

Summary of decisions:

1. Commissioners to provide comments with respect to the draft set of technologies and methods attached to these minutes (and questions to be asked with respect to these technologies and methods) by July 31.
2. Report Subcommittee to provide on August 4: (a) questionnaire re final set of technologies and methods and questions to be asked; (b) sample responses to one portion of questionnaire to show how process will work; (c) annotated outline of report with proposed table of contents; (d) proposed schedule for post-August 4 report meetings; and (e) proposed plan for small group meetings.

3. Commissioners to respond to questionnaire and provide an informal memo with respect to their overall positions (and initial proposed recommendations, if any) by August 18.

Chairman Telage stated that the report presents the Commission with a difficult challenge. Staff has been thinking through the problems presented by the report. Chairman Telage noted that even if the Commission receives no public funding (and only small amounts of private funding) a significant number of meetings will be needed for the Commission to reach consensus on its recommendations.

Chairman Telage asked the Commissioners to read through the COPA sections dealing with the report, and asked the Commissioners to focus on the charter given them by Congress.

Chairman Telage noted that the report needs to be finished by October 1. This means that (given August vacation schedules), the Commission has just one month to write its report.

Commissioner Vradenburg asked how many commissioners were needed to agree on the report to allow it to issue. David Johnson said that the statutorily-defined quorum (nine commissioners) needed to be present for the Commission to act. It was agreed that a majority of the statutory quorum (or five of nine commissioners) would need to agree to approve the report. Commissioner Flores noted that the Commission could adopt any rules it needs to allow it to operate.

Chairman Telage moved to a discussion of a draft recommendation dated July 17 prepared by his staff (attached). He noted that the Report Subcommittee had not approved any aspect of this draft recommendation, and that it was merely a suggestion of a way to proceed.

David Johnson, on behalf of Chairman Telage, discussed the draft recommendation. He noted that if the Commission took seriously its need to analyze each technology and method discussed during the hearings with respect to all the questions raised by Congress in COPA, this would be a very large task. Johnson said there was a need to (a) consolidate sets of technologies and methods and to (b) settle on the questions that would be asked with respect to these technologies and methods.

Chairman Telage asked that Commissioners provide comments with respect to the July 17 draft set of technologies and methods (and questions) by the close of business on July 31.

Commissioner Rice Hughes noted that the staff of FamilyClick had agreed to collect and organize the answers to the filtering/labeling questionnaire sent out by the Hearing 2 organizers.

David Johnson said that it would be necessary to do as much work as possible on the report during August. The July 17 draft contemplated a three-stage process: (1) analyze technologies and methods; (2) present and debate recommendations; (3) draft individual statements and prepare the report, including appendices. Given the shortness of time, it would make sense to start the recommendation drafting process during August. This would provide useful input for the analysis of technologies and methods, and would allow Commissioners to see where consensus was emerging and where there was need for further discussion.

Chairman Telage emphasized that the report would have three sections following any executive summary: a set of voted-on recommendations, approved with supporting documentation; an analysis of the technologies and methods with respect to their effectiveness and costs and adverse impacts (obtained by ranking factors on a scale of 1-10), presented in a graphical fashion accompanied by explanatory text; and individual statements, open-ended but limited in length. Chairman Telage noted that the development of the report will require the Commission to interact in a way it has not yet done. An alternative way to proceed would be to get staff going on a draft report, edit it collectively, and then have Commissioners sign on. Chairman Telage noted that this method might be easier but would not be as useful to Congress.

Commissioner Vradenburg said that he believed it would make sense for staff to begin by preparing an annotated outline and table of contents in preparation for the August 4 meeting of the Commission. He noted that he had thought at first that the analysis of technologies and methods proposed by the Chairman's staff was too complex, but that he now believes that this process will be valuable to show agreement and lack of agreement. Commissioner Vradenburg suggested that both processes (report drafting and analyses) occur simultaneously.

Chairman Telage supported the idea of an annotated outline. He asked that the Report Subcommittee provide the Commission with sample sections of the report.

Commissioner Vradenburg said that a table of contents and outline would be essential to provide some sense of context for the issues faced by the Commission.

Commissioner Berman suggested that the Report Subcommittee prepare trial analyses of technologies and methods, and provide the Commission with sample narratives regarding what was meant by the ratings provided. Such a sample will assist the Commission in developing talking points and support for (or opposition to) particular recommendations, and will avoid confusion when open discussion begins.

Commissioner Talbert noted that it would be helpful to request recommendations from witnesses.

Commissioner Balkam suggested that in light of the shortness of time a Commission retreat in early September would be useful. He also noted that he and others will not be available on September 8 (and days close to that date) due to a meeting in Germany.

Chairman Telage noted that the Commission should decide whether to schedule such a retreat in light of the Commission's lack of funds.

Commissioner Vradenburg requested that each Commissioner provide in response to the questionnaire concerning technologies and methods a memo summarizing their initial positions or feelings with respect to the overall questions presented to the Commission. Commissioner Schmidt added that this initial memo should include plausible outcomes or recommendations for the Commission to consider.

Chairman Telage said that the Report Subcommittee would provide an agreed-upon list of technologies and methods (and questions) by August 4. Based on that list, staff will send to the Commissioners a voting template. Commissioners should respond with any textual comments they have in addition to their votes, and include a statement regarding their view of what the Commissioners should do. The deadline for responses to the questionnaire/template will be August 18.

Commissioner Berman expressed a wish to speak off the record about the Commission's work and have candid discussions. Commissioner Rice Hughes said that it would be helpful to have small groups for private discussions. David Johnson said that the Report Subcommittee would provide suggestions for smaller groups. Chairman Telage noted that the Report Subcommittee would also suggest a timeline for meetings following August 4. The report will take at least two weeks to produce, and the Commission must audit its finances before dissolving.

Hearing 2

The Commission briefly discussed Hearing 2. Commissioner Telage noted that the time structure of the hearing had presented challenges. Commissioner Parker noted that the quality of the witnesses had differed widely, and that organizers needed to make sure that Hearing 3 witnesses provided real data and information. Commissioner Balkam agreed to stress the five minute rule and to ask for figures. Commissioner Flores suggested that Chairman Telage interrupt witnesses if they are running over time.

The meeting adjourned at approximately 3:15 p.m.

Commission on Child Online Protection
Meeting Minutes
August 4, 2000

Present: Commissioners Telage (chair), Rice Hughes, Vradenburg, Berman, Parker, Horowitz, Ganier, Flores, Bastian, Balkam, Schmidt, Talbert, Peeler, DeRosier and Srinivasan.

Sallianne Fortunato sat in for Commissioner Greg Rohde.

Meeting began at 12:10 p.m. PST

Chairman Don Telage discussed the methodology for writing the report to Congress. He explained the evaluation criteria. Chairman Telage asked all the Commissioners to fill out the questionnaire and score it against the technology and methods document. As part of the questionnaire, Commissioners will have the opportunity to make recommendations to Congress.

He also asked each Commissioner to write a personal statement about their observations and recommendations.

Chairman Telage said that this first round of data will serve as a straw man poll so that Commissioners will know where each Commissioner is coming from at the September report writing meeting.

Commissioner Rice Hughes suggested adding several additional technologies and methods to the list to be evaluated. Chairman Telage agreed to revise the document.

Commissioner Berman suggested ways to fill out the questionnaire, saying it is easier if you write the reasons for answering question the way that you did next to each question.

Commissioner Vradenburg asked if the Commission's recommendations should only focus on "harmful to minor" material. He said that issues such as predation, pornography and obscenity bear relationship to but don't directly fall beneath harmful to minor's materials.

Chairman Telage answered that the Commission should stick to its original mission and fulfill our mandate. He said that some panels in hearing 3 did go beyond our scope and that these issues can be included as peripheral in our report.

Chairman Telage noted that once the original statute is met, the Commission could include more in its report to Congress.

Commissioner Berman questioned if limited resources are diverted from most hard-core cases to harmful to minor's material then are we really hurting the overall issue.

Commissioner Flores said that individual Commissioners could include observations that the Commission as a whole does not agree on in the personal statement

Questionnaire

Chairman Telage advised the Commissioners how to answer the questionnaire. He said to fill out the ratings matrix as they are reading the questionnaire. He also stressed the importance of including comments because they will help later with the discussion of why commissioners assigned the values they did.

The data is due to Kristin Litterst by August 18.

Chairman Telage also asked Commissioners to begin working on personal statements so that each commissioner understands the differences in position.

Commissioner Flores stated that Commissioners have the right to withhold personal statements until they are ready to submit.

Chairman Telage committed to making changes to the outline and questionnaire and resending the materials to the Commission on Monday, August 7. He also announced that Rocky Mountain College will serve as the Commission's fiscal agent.

Chairman Telage said the Commission must assume that we will not receive congressional funding. If the Commission is extended and funded then the Commission could issue an interim report in October. If the Commission was granted an extension, then the Commission would continue work on the report and resubmit it.

Commissioner Rice Hughes suggested keeping a running list of what the Commission would like to do if granted more time.

Commissioner Berman suggests giving this list to Congress as an example of why the Commission needs funding and more time to fulfill its mission.

Commissioners Schmidt and Berman believe further consideration should be taken before issuing an interim report.

Meeting September 12-13 in the Washington, DC area. (*meeting date confirmed for September 18-19 pursuant to a vote by the Commission*).

Commissioner Berman asked each Commissioner to take assignments to contact House and Senate conferees. He discussed presenting a unified message to each congressional staffer.

Several questions were asked about the Commission's funding.

Commissioner Flores said that gifts to the Commission are tax deductible, but only if the money is not returned if the Commission receives funding.

Chairman Telage asked that the letters be sent to Members of Congress the week of August 7. He also said that he is making a list of companies from whom to ask for donations to the Commission.

The meeting adjourned at 2:00 p.m. PST

COPA Commission

Information and Resources About the Commission on Online Child Protection (COPA)

Hosted by the Congressional Internet Caucus Advisory Committee

Agenda of the Commission on Online Child Protection (COPA) meeting

The Commission on Child Online Protection (COPA) Meeting
September 18 - 19, 2000

Date and Time:

Monday, September 18, 2000 9:00 a.m. - 5:00 p.m.
Tuesday, September 19, 2000 9:00 a.m. - 5:00 p.m.

Location:

1425 New York Avenue N.W.
Penthouse Floor (PH), Office of the Chief, Room13044
Conference Room #13083 (follow the posted signs)
Washington, D.C. 20005
A photo i.d. is necessary to enter the building due to tight security measures.

Monday, September 18

9:00 a.m.

Opening remarks from Don Telage, Chairman, COPA Commission

9:15 a.m. - 9:45 a.m.

Presentation on report-writing process, Don Telage

9:45 a.m. - 12:00 p.m.

Review and discuss questionnaire

12:00 p.m.

Working lunch

12:00 p.m.- 5:00 p.m.

Review and discuss questionnaire

BEST COPY AVAILABLE

5:00 p.m.

Adjourn

Tuesday, September 19

9:00 a.m.

Welcome by Don Telage

9:30 a.m. - 12:00 p.m.

Review and discuss questionnaire
Discuss report draft and recommendations (as time permits)

12:00 p.m.

Working lunch

12:00 p.m.-5:00 p.m.

Review and discuss draft report language
Discuss report draft and recommendations (as time permits)

5:00 p.m.

Adjourn

[Home] [Final Report] [About this Site] [FAQ] [The Commission] [Press Room]
[Meetings and Hearings] [Research Papers] [Privacy Policy]

webmaster@copacommission.org / Copyright © 2000

COPA Commission
Information and Resources About the Commission on Online Child Protection (COPA)
Hosted by the Congressional Internet Caucus Advisory Committee

Minutes of the Child Online Protection Act (COPA) Commission meeting

September 18-19, 2000

Present: Commissioners Telage (chair), Balkam, Bastian, Berman, DeRosier, Flores, Ganier, Horowitz, Parker, Peeler, Rice Hughes, Rohde and Talbert.

Liza Kessler sat in for Commissioner Vradenburg, Claudette Tennant sat in for Commissioner Schmidt, and John LoGalbo sat in for Commissioner Schrader.

The meeting, which was held in Washington, D.C., began at 9:20 a.m. EST

The Commission reviewed draft introductory language for the report to Congress. The Commissioners then discussed, in sequential order, the different technologies and methods contained in a questionnaire that was filled out by the Commission prior to the meeting. The Commissioners discussed their scores and engaged in constructive debate over the 17 technologies and methods.

The technologies and methods include:

Common Resources and Parental Education

1. Online information resources
2. Parent Education Programs

Filtering/Blocking

3. Server-side filtering using URL lists
4. Client-side filtering using URL lists
5. Filtering (server- and client-side) using content analysis

Labeling and Rating Systems

6. First-party labeling/rating
7. Third-party labeling/rating

Age Verification Systems

8. AVS based on credit cards
9. AVS based on independently-issued ID

BEST COPY AVAILABLE

New Top-Level Domain/Zoning

10. Establishment of a gTLD for HTM content
11. Establishment of a gTLD for non-HTM content
12. Establishment of a "green zone" or "red light zone" by means of allocation of a new set of IP numbers
13. Hotlines/Warning systems

Other Technologies and Methods

14. Greenspaces
15. Monitoring and time-limiting tools
16. Acceptable use policies/family contracts
17. Increased prosecution

The Commissioners added an 18th technology, "Real Time Content Monitoring/Blocking" to the technology and method list.

The Commission then reviewed draft recommendations to Congress that were written by individual Commissioners. Several of the recommendations were consolidated and individual Commissioners took responsibility for drafting recommendations that will be reviewed at the October 4-5 meeting at America Online, Inc. in Sterling, Virginia. The Commission also discussed reviewing a draft of the entire report at the October meeting.

The meeting adjourned at 5:00 p.m. EST on September 19, 2000.

[Home] [Final Report] [About this Site] [FAQ] [The Commission] [Press Room]
[Meetings and Hearings] [Research Papers] [Privacy Policy]

webmaster@copacommission.org / Copyright © 2000

COPA Commission

Information and Resources About the Commission on Online Child Protection (COPA)
Hosted by the Congressional Internet Caucus Advisory Committee

Agenda for the October 4-5 Commission on Online Child Protection (COPA) meeting

Date and Time:

Wednesday, October 4, 2000
9:00 a.m. - 5:00 p.m.

Thursday, October 5, 2000
9:00 a.m. - 5:00 p.m.

Location:

America Online, Inc.
22200 AOL Way
Sterling, VA 20166
(703) 265-3000
"The Paris Room"
Please bring a photo I.D. for entry into the building.

Agenda:

Wednesday, October 4

9:00 a.m. Opening remarks from Don Telage, Chairman, COPA Commission

9:15 a.m.-noon Review and discuss draft recommendations

12:00 p.m. Working lunch

12:00 p.m.- 5:00 p.m. Review and discuss draft report language

5:00 p.m. Adjourn

Thursday, October 5

BEST COPY AVAILABLE

9:00 a.m. Welcome by Don Telage

9:15 a.m. - 12:00 p.m. Discuss report language and recommendations

12:00 p.m. Working lunch

12:00 p.m.-5:00 p.m. Vote on report language and recommendations

5:00 p.m. Adjourn

**During the meeting, there will be time to adjourn so small groups of Commissioners can discuss, refine and gather support for recommendations.

[Home] [Final Report] [About this Site] [FAQ] [The Commission] [Press Room]
[Meetings and Hearings] [Research Papers] [Privacy Policy]

webmaster@copacommission.org / Copyright © 2000

COPA Commission

Information and Resources About the
Commission on Online Child Protection (COPA)
Hosted by the Congressional Internet Caucus Advisory Committee

Official Hearing Notice May 24, 2000

Request for Comments on "One-Click Away" Resources, Age Verification Systems and Creation of an Adult Domain

ACTION: Hearing announcement and request for submission of comments in preparation for hearing of the Commission on Online Child Protection.

SUMMARY: The Commission on Online Child Protection (the COPA Commission) was directed by Congress in the Child Online Protection Act (COPA), 47 U.S.C. Sec. 231, to conduct a study regarding methods and technologies to help reduce access by minors to material on the World Wide Web that is harmful to minors. As part of this review, the Commission has scheduled three public hearings to consider these methods and technologies. On June 8-9, 2000, the COPA Commission will hold the first such public hearing in Washington, D.C. to consider "one-click away" resources, age verification systems, and creation of an adult top-level domain. Today's notice seeks comments on these methods and technologies.

DATES: Submissions are requested by **June 2, 2000**, in order to permit consideration in advance of the hearing.

ADDRESSES: Comments should be submitted in electronic form, to following email address: comments@copacommission.org. The subject line for all submissions should read: "Comments on First Hearing Subjects."

FOR FURTHER INFORMATION CONTACT:
Kristin Hogarth Litterst
Dittus Communications Inc.,
1000 Thomas Jefferson St, NW #311
Washington, DC 20007
202-298-9055
comments@copacommission.org (for questions or information)

The Child Online Protection Act, 47 U.S.C. 231 note, ("COPA"), as amended, established a temporary, 19-person Commission to study methods and technologies to help reduce access by minors to material on the World Wide Web that is harmful to minors. The COPA Commission is directed to submit a report to Congress, no later than October 21, 2000, on the results of this study, including:

> **a)** a description of the technologies and methods identified by the study and the results of the analysis of each such technology and method;
>
> **b)** the conclusions and recommendations of the Commission regarding each such technology or method;
>
> **c)** recommendations for legislative or administrative actions to implement the conclusions of the Commission, and
>
> **d)** a description of the technologies or methods that may meet the requirements for use as affirmative defenses to liability for purposes of section 231(c) of COPA.

The COPA Commission will hold three public hearings. On June 8-9, 2000, it will hold a hearing at the Federal Trade Commission, 600 Pennsylvania Avenue, N.W., Washington, D.C., Room 432, on "one-click-away" resources, age verification systems, and creation of a top-level adult domain, such as .xxx or .adult domain. On July 20-21, 2000, it will hold a hearing on filtering and labeling systems, at a location to be determined. On August 3-4, 2000, it will hold a hearing on other technologies and methods, at a location to be determined.

Information solicited by this notice: [redacted]

In connection with the first public hearing, the COPA Commission asks the public to submit comments on "one-click-away" resources, age verification systems, and creation of an adult domain. Comment is sought on any issue of fact, law or policy that may have bearing upon the COPA Commission's report insofar as it concerns these technologies.

The following are questions that may be considered at the June 8-9 hearing:

Common Resource(s) for parents to use to help protect minors (such as 'one-click-away')

- How often is the resource used?
- How often is the resource updated?

- In what particular ways does the resource assist parents?
- Is there any data regarding satisfaction of those who use the resource?
- How is the resource marketed or promoted?
- Does the resource help prevent access by children to web sites with materials harmful to minors?
- Does the resource help prevent problems associated with incoming email?
- What percentage of those who use the resource go on to select and use specific tools it identifies?
- Does the resource provide assistance to companies offering blocking or filtering services?
- What could be done to make it easier to locate the resource?
- What if anything could be done to increase usage of the resource?
- What if anything could be done to make the resource more effective?
- Should the availability of the resource be considered to provide a defense to prosecution under COPA?
- Does the resource provide any assistance to law enforcement?
- Does use of the resource create any data that implicates privacy rights?
- Does the existence of the resource raise any first amendment issues?
- Does the availability of the resource increase the likelihood that parents who wish to do so will be able to restrict access by their children to materials harmful to minors?
- What other information might usefully be included in a common resource?
- Are there legal or other barriers to the sharing of useful information via this common resource?
- Is there a business model that assures continued availability and enhancement of this common resource?

- Would governmental action to subsidize or regulate this common resource raise first amendment or other issues?
- What reason is there to believe that any problems in parental adoption of various technologies or methods or restraining access by their children are due to lack of information or other tools that would be provided by a common resource?
- Could the resource be made more readily available or more easily used if it were tied into the browser in some more direct way (e.g., as an always-visible icon)? Do you have reason to believe that the Internet industry would support creation of something like an always-visible icon? Should the government require browsers or operating system software to include such an icon?
- Should web sites with material harmful to minors be required to link to such a common resource?
- Should restrictions on unsolicited email be relaxed with respect to messages advertising such a resource?
- What evidence is there regarding the extent to which Internet using parents are actually aware of the resource?
- If the resource lists safe sites, are those listings accurate and up to date?
- What percentage of parents wants to limit their children's access to only safe sites listed in such a resource?
- Is there a technological means of assuring that a child only has access to the listed safe sites?
- What kinds of useful material would be rendered unavailable to children if only listed safe sites could be visited?

Establishment of a [top level] domain name for any material that is harmful to minors

- Who would (or can) make the decision to establish such a domain name?
- If the domain were voluntary, would it attract HtM web sites? How?
- How would such a domain be used in connection with specific pages of web sites that were HtM, where the rest of the site is not HtM?

- If use of the domain were mandatory, would this raise significant first amendment issues?
- If US law required use of the domain, would this lead HtM sites to move offshore?
- What percentage of HtM sites would likely move to the new domain?
- Would use of this domain make filtering more effective?
- How would use of such a domain relate to email?
- What would be the costs to web sites of relocating to such a domain?
- Would such a domain create an attractive nuisance that made it easier for children to find HtM materials?
- Would any of the above analysis differ depending on whether the domain were a top level domain, a second level domain, or some other level of domain?
- What would prevent creation of deep links to pages within such a domain from web pages outside the domain?
- Is it desirable to prevent deep links to pages within such a domain from web pages outside the domain?
- Would creation of such a domain eliminate any need for age verification?
- Should use of such a domain provide a defense to a charge under COPA?
- Would creation and use of such a domain raise privacy issues?
- If use of the domain were mandatory, how would such a law be enforced?
- How would web sites determine whether they should or must put particular materials into the new domain?
- Would materials from the new domain show up in results produced by net search engines?
- What would reasonably be projected re the impact of such a domain on adoption by parents of filters that filter out sites in the domain?
- What would be the implication of creation of a domain designed to

hold only NON-HtM materials (e.g., .kids?)

Age Verification systems

- Does the system accurately identify any user as over a certain age?
- How does the system accurately identify any user as over a certain age?
- Is use of the system merely to verify age allowed?
- How widely available is the system to end users?
- How much does it cost end users to use the system?
- How much does it cost a web site to use the system?
- How easy is it for children to obtain false age identification for use online?
- How easy is it for parents to monitor their children's use of the system?
- Does the system allow differentiation or distinction with regard to children of different ages?
- Do systems now in use substantially impact access by children to HtM material?
- Should use of the system by a web site provide a defense to a COPA charge?
- Does the use of such a system create threats to privacy?
- Does the use of such a system comply with COPPA?
- Would mandatory use of the system raise significant first amendment issues?
- Does use of the system assist or detract from law enforcement in any way?
- Should use of the system be made mandatory for users? For web sites?
- Can the system be tightly integrated with web browsers?
- Does use of the system have implications for system security?

- How does the system relate to web use in libraries? From work?
- Is there any way to derive a good inference of age from data regarding a user and his or her net use that is already available and accessible by a web site?
- What is the likely evolution of certificates, passports, biometrics and other net identifiers independent of the HtM issue? Does this have implications for the questions facing the Commission?
- How does the burden of adopting age verification technology compare with the burden of self-labeling by web sites with HtM materials?

Comments filed with the COPA Commission will be made available to the public. Comments filed by 5:00 p.m. on June 2, 2000 will be made available to the COPA Commissioners for consideration in advance of the hearing. The record will remain open for further public comments until a date to be announced at the last of the three hearings.

In an upcoming notice, the COPA Commission will make public the agenda for the June 8-9 hearing.

---

webmaster@copacommission.org / Copyright © 2000

COPA Commission

Information and Resources About the
Commission on Online Child Protection (COPA)
Hosted by the Congressional Internet Caucus Advisory Committee

Guidelines for Submitting Public Comments

Since the Commission has completed its work, no more submissions can be accepted. Questions about Commission activities may be addressed to comments@copacommission.org.

[Home] [Final Report] [About this Site] [FAQ] [The Commission] [Press Room]
[Meetings and Hearings] [Research Papers] [Privacy Policy]

webmaster@copacommission.org / Copyright © 2000

BEST COPY AVAILABLE

COPA Commission

Information and Resources About the
Commission on Online Child Protection (COPA)
Hosted by the Congressional Internet Caucus Advisory Committee

AGENDA AND WITNESS LIST FOR COPA COMMISSION HEARING

June 8-9, 2000, Federal Trade Commission in Washington, D.C.

June 8: Common Resources For Parents and One-Click-Away Resources

9:30 a.m. - 9:45 a.m. **Introductions**

Welcome by Chairman Telage, Subcommittee Co-Chairs Commissioners Berman and Flores

9:45 a.m. - 10:45 a.m. **"One-Click -Away" and Other Common Resources**

- GetNetWise case study
  - Jim Browne, Director, GetNetWise *biography* *testimony*
  - David Eisner, Co-Chair, GetNetWise/AOL *biography* *testimony*
  - Marilyn Cade, Co-Chair, GetNetWise/AT&T *biography* *testimony*
- Parry Aftab, Executive Director, Cyberangels.org *biography* *testimony* *testimony 2*

10:45 a.m. - 11:00 a.m. **Break**

11:00 a.m. - 11:30 a.m. **Other Common Resources and Analysis**

- Ernie Allen, President, Nat'l Center for Missing and Exploited Children *biography* *testimony*
- Larry Magid, SafeKids.com *biography* *testimony*

11:30 a.m. - 12:00 p.m. Comment Period

12:00 p.m.-1:30 p.m. Break for Lunch

June 8: Top Level Domain

1:30 p.m. - 2:30 p.m. **Feasibility**

- Roger Cochetti, Senior V.P. and Chief Policy Officer, Network Solutions *biography testimony*
- Jonathan Weinberg, Professor of Law, Wayne State University *biography testimony*

2:30 p.m.- 2:45 p.m. **Congressional Perspective**

- Senator Joseph Lieberman, *biography testimony Attachment*

2:45 p.m. - 3:00 p.m. Break

3:00 p.m. - 4:00 p.m. **Analysis and Policy Implications**

- Bruce Watson, President, Enough is Enough*biography testimony Attachment*
- Bob Corn-Revere, Hogan & Hartson *biography testimony*
- April Major, Former Law Professor, Villanova Law School *biography testimony*
- Bruce Taylor, President and Chief Counsel, National Law Center for Children & Families *biography testimony*
- David Post, Temple University Law School & George Mason University *biography testimony*

4:00 p.m. - 4:30 p.m. Comment Period

June 9: Age Verification Technologies

9:30 a.m. - 9:45 a.m. **Introductions**

Welcome and Opening Remarks by Chairman Telage, Subcommittee Co-chairs Commissioners Berman and Flores

9:45 a.m. - 12:00 p.m. Feasibility, Analysis and Policy Implications

- Mark MacCarthy, Senior Vice President for Public Policy, VISA U.S.A. *biography testimony*
- Michael Baum, VP, Practices and External Affairs, VeriSign, Inc. *biography testimony Attachment*
- Pat McGregor, Chief Information Security Architect, Intel *testimony*
- Biometrics Overview
  - John Woodward, Senior Policy Analyst, RAND *biography testimony*
  - Jeffrey Dunn, Co-chair Biometric Consortium *biography testimony*
  - Fernando Podio, Co-chair Biometric Consortium *biography testimony*
- David Sobel, General Counsel, Electronic Privacy Information Center *biography testimony*

11:00 a.m. - 11:15 a.m. Break

12:00 p.m. - 12:30 p.m. Comment Period

[Home] [Final Report] [About this Site] [FAQ] [The Commission] [Press Room]
[Meetings and Hearings] [Research Papers] [Privacy Policy]

webmaster@copacommission.org / Copyright © 2000

Jim Browne
Director, GetNetWise

Mr. Browne has served in a number of capacities prior to directing GetNetWise. At the Communications Consortium Media Center (CCMC) he served as Director of New Initiatives. The Consortium serves to make both electronic and print media available to nonprofit organizations and collectively help them use "strategic media" to advance common issues. At CCMC Mr. Browne managed development activities, worked with other senior staff to coordinate projects, and to launch the Coordinated Campaign for Learning Disabilities, a major effort to recognize and address learning disabilities in children. He also served as director of the Projects Program of the Tides Foundation and the first director of its eastern office. Previously, Mr. Browne as the senior program office of the Field Foundation of New York where he focused on youth development, voter participation, and issues of civil liberties. Mr. Browne was also a senior fellow at the Robert F. Kennedy Memorial where he helped to conduct an inquiry in the state of high school journalism for the Memorial.

COPA Commission Hearing

June 8, 2000

Introduction

It is a pleasure for us to be here before the COPA Commission and to discuss GetNetWise a comprehensive toolbox of resources for parents that is widely distributed online. GetNetWise is a direct response to the serious need to protect children online from unwanted and inappropriate content or contacts. On the Internet, GetNetWise is designed to be easy to use and easily accessible "one click away." That powerful click is the response to a challenge to the Internet industry to help families keep their children safe online while affording them the opportunity to take full advantage of the learning and recreational potential of this global medium.

GetNetWise is a direct response to the Internet medium – a world wide network, without borders or centralized points of control. The Internet is not physically contained within the jurisdiction of a locality, state, or nation, nor subject to the laws of any one nation. It is an open medium, in which people all over the world determine the course of their own online activities, viewing and creating content. A click on a link can send content racing from a computer half way around the world, jumping oceans as easily as city lines.

Who exercises control of this content? No one, and everyone. No one has the means to control, or limit, or legislate what the world will put on the World Wide Web. But everyone has the means to limit what comes in to his or her own computer. The power to control content lies with the end users. And when the end users are children, control should lie with parents or caregivers.

Parents are finding that with one click of a mouse, they can gain access to information needed to help ensure that the Internet is an educational and entertaining world for their children to explore, safe from unwanted and inappropriate content or contacts. That

powerful click is the response to a challenge to the Internet industry, to help families keep their children safe online.

The challenge embraced by GetNetWise is two-fold: first, to assemble information about the use and deployment of online empowerment tools into a common, easy-to-use resource for parents, and second, to ensure that the resource has the widest distribution possible, so that it is essentially one click away.

Both Congress and the Administration worked with Internet industry leaders and well-known family groups in the 1997 Internet Online Summit and the 1998 America Links Up campaign to address children's safety online. Since then, the Internet industry has focused on creating a collection of resources that would be accessible from the major entry points to the Internet and that would provide families with information on how to guide their children online. The Child Online Protection Act (COPA) asked whether providing one click access to such a common resource for parents was feasible. Before the COPA Commission even convened to examine this question, a partnership of Internet companies and public interest groups came together with the goal to create just such a resource.

The partnership, which includes AOL, AT&T, Alta Vista, Bell Atlantic, Bell South, Cyber Patrol, Dell, Disney Online, EarthLink, Excite@Home, IBM, Lycos, WorldCom, Microsoft, Net Nanny, Network Solutions, Prodigy, Road Runner, Surf Watch Software, Yahoo!, Zeeks, the American Library Association, Association of American Publishers, Center for Democracy and Technology, Center for Media Education, The Children's Partnership, Commercial Internet eXchange, Cyberangels, Enough is Enough, Internet Alliance, Internet Content Rating Association, National Center for Missing and Exploited Children, NetFamilyNews, People for the American Way, and the US Chamber of Commerce, believes that this goal was reached when GetNetWise was launched in July, 1999, demonstrating that one-click away access was not just feasible, but operational. For the past ten months, it has been helping parents keep children safe by giving them the means to guide their children's online activities. Parents need only to access the child

safety page on their Internet Service Provider (ISP), Online Service Provider (OSP), or portal site, and they will be but one click away from the resources that the partnership has made available on GetNetWise.

Why GetNetWise?

GetNetWise offers parents and caregivers the most effective technological and legal means by which they can protect their children from unwanted and age-inappropriate content on the Internet.

Through GetNetWise, a public service sponsored by Internet companies and public interest organizations, families can find the means to exercise that power in their own homes, making the Internet a safe and valuable resource for their kids. GetNetWise is more than a Web site. It represents a commitment to child safety from ISPs, OSPs, and portals. These companies, which serve as gateways to the Internet for over 90% of Internet users in the country, have given parents one-click access from their sites to family-friendly information and tools for online safety.

As the Internet grows, it is augmenting or supplanting other media such as newspapers, television and radio. Parents and educators realize that denying children access to the Web, and all the benefits that access confers, is a great risk—though certainly not the only one. As children plunge into an array of educational, entertaining, and wholesomely engaging resources, they may come upon other, objectionable material. At GetNetWise, we know that the best way to have kids be safe users is to empower their parents to guide their Internet explorations and help them make good choices, based on their family's values and the child's ages and maturity.

Establishing guidelines and standards can be a challenge for parents. Often parents are less familiar with Internet technology than their children. While parents may make little or no use of the Internet, many children are using it in school or in the library, and are even becoming Web authors as their own class projects are posted to school Web pages.

Often they use the Internet at home without adult supervision. Parents who want to understand the alternatives available to them to help their children stay safe online find GetNetWise to be a valuable resource.

What makes GetNetWise so useful? First, accessibility: Over 90% of online users have one-click access through their ISP, OSP, or popular portal sites, via a button or link which connects them directly to GetNetWise resources. Second, we help parents understand the nature of the risks that their children face online, and suggest actions they can take in response. Third, we offer a list of recommended sites appropriate for children, and finally, we give parents access to tools which will help them make their children's online experience safe and enriching. GetNetWise is regularly updated so parents can be assured that the information they are getting is current.

What kind of helpful information will parents find through GetNetWise?

GetNetWise provides four types of information:

- **Online Safety Guide**

  The Safety Guide provides information about the potential safety and privacy risks to children online. In a frank but friendly tone, the guide helps parents learn about the kind of material available on the Internet, and what issues merit their concern. It explains that the primary appeal of the Internet, interactivity, is also the attribute which creates the greatest risk. But what's new to parents may already be second nature to children; parents may find they're learning things their children already know.

  Because one solution doesn't fit all children or all families, the safety guide addresses the needs of children by age/maturity level, and offers general tips for children, teens, and families. It also covers specific risks, and offers strategies to deal with each. In some situations, technology may offer parents a way to solve a particular problem;

when that is the case, a link can take parents directly to Tools for Families, where they can learn about the tool and what it can do for them.

- **Tools for Families**

The tools section provides a comprehensive directory of over 110 technology tools that families can use to filter, block or monitor access to inappropriate content, such as violent or sexually explicit materials. The directory also includes tools which filter, block, or monitor outgoing materials, such as e-mails or chat rooms where children might post information. Parents can learn about the different ways that these tools work, and the standards that they apply, to determine what tools will work best for their family. These tools can be changed or altered as kids grow up and can be personalized to each computer and each user in the house. A searchable database allows parents to identify their needs and see a list of appropriate tools. Links to the tool providers allow parents to download the latest versions.

Because we want parents to have as much information as possible about available technology, we add new tools to the GetNetWise database when they are made available. We keep the database current by actively looking for new tools, and we provide an online request that developers can use to tell us about their new family empowerment software. The criteria for inclusion on the tools directory are posted, and of course, there is no charge to the software companies for the listings. Currently, there are more than 110 tools listed in the directory.

Interestingly, one of the frequently viewed tools is not a technological solution at all, but a sample contract or agreement, which sets out in simple language the rules that a child agrees to follow when going online. The child pledges to follow the rules that minimize his or her risk, and to keep parents or caregivers informed if anything untoward happens. Links to other such contracts are also provided.

- **Reporting Trouble Online**

For many parents, the first indication that they need to be involved in their child's online activities comes when they see that a child has accessed inappropriate or objectionable materials. In a panic because their child has been exposed to pornography or other pernicious content, they may assume that a law has been broken. This section of GetNetWise helps parents understand the difference between material that is illegal and material that is inappropriate for their child, and between what is dangerous and what is merely annoying.

More important, it provides information on what steps to take in response to various situations, from calling law enforcement if a child's safety is immediately threatened to reporting sites which include illegal material. Should the situation warrant a call to law enforcement, links are provided to state police and to federal law enforcement agencies. These agencies can provide comprehensive advice about dealing with online problems. Additionally, there are links and/or phone numbers for child advocacy organizations involved with various threats to children, in both the online and physical worlds.

- **Web Sites for Kids**

Parents often look to "Kid-Safe" Web sites to provide a safe and enjoyable online haven for their children. Our list includes current sites that have been developed or recommended by our partners or by other family-oriented non-profit groups and child development experts.

Parents need options based on their values and the needs of their children. Some may choose to use tools which will limit their children's viewing to sites such as these or other kid-oriented sites. But, as they learn when they read about blocking and filtering technology, they may be restricting their children's access to valuable and appropriate information. A young girl entering puberty, for example, may seek information about the changes her body is undergoing, but find that any mention of reproductive organs has been screened from the content she is permitted to see. As children grow up, their

information needs change, and GetNetWise can give their parents the resources they need to make decisions about their child's online access.

How have parents been made aware of GetNetWise?

The July, 1999, launch of GetNetWise generated widespread coverage, reaching millions of American homes through television, radio and print media. Attendance of key policymakers, corporate executives, and other well-known supporters at the launch ensured coverage in all top ten television markets, as well as 50 smaller markets. C-Span coverage and rebroadcasts, video news releases and repackaged news releases continued to enlarge the number of viewers reached. Print coverage by the *New York Times, Washington Post, USA Today, Christian Science Monitor, Los Angeles Times*, and the wire services extended the story, as did coverage by online zines such as C/Net, Newsbytes, PCWeek Online, ZDNet, and others.

Since the launch, GetNetWise and its partners have continued to earn media coverage in connection with safety for children online. We have promoted the site in a variety of ways, including banner ads and buttons displayed on the Web, bookmarks distributed at libraries, print brochures distributed at trade shows for educators, advertisements on bags of Wise Potato Chips, and promotional video screens displayed at 7-11 Stores. Information about GetNetWise is included in briefings of policymakers and public officials at federal, state, and local levels.

Partners and supporters provide one-click linkage to the GetNetWise site (or their own functional equivalent site) from their own Web sites, and they often promote the site in other ways. For example, AT&T gives the logo a prominent position, has included the site in an online shopping guide for consumers, and listed it as a resource on their "Parents" page. Lycos distributes GetNetWise capability brochures at all events attended by Lycos Zone, including trade shows pertinent to children and educators, and information about GetNetWise is included in Lycos Zone press kits at shows and press events. Microsoft runs banner ads on MSN, and includes information about GetNetWise

in appropriate press announcements and online feature stories. The National Center for Missing and Exploited Children and Net Nanny introduce and promote GetNetWise at classes conducted for law enforcement, parents, and teachers.

Interest in online safety and potential solutions for parents has filtered from the technology world into the mainstream, increasing the visibility of GetNetWise. No longer just the purview of technology writers, online safety is now addressed by journalists who cover education, family issues, children, and consumer affairs. References to GetNetWise have recently appeared in articles about privacy, as well as in an article about how parents are finally taking cues from their children and using the Internet to trade parenting tips. A recent episode of CBS Television's "Touched by an Angel" dealt with online safety, and referred viewers and Web site visitors to Enough is Enough, the National Center for Missing and Exploited Children, and Safekids.com, all GetNetWise advisors.

How are parents responding to GetNetWise?

- **Traffic**

During the first ten months since GetNetWise came online, it provided 1,746,538 online users access to this resource, representing more than 12 million hits. Also, these numbers do not include page views by those partners, particularly Yahoo!, that provide their own version of GetNetWise resources tailored for their audiences.

Information from our partners indicates that online child safety resources generate a great deal of traffic. But understandably, not all of our partners tally the visits to their child safety pages, and those who do may count them differently. Some have numerous features bundled into their child safety pages, which makes extraction for purposes of assessing their link to GetNetWise impossible. Net Nanny, for example, a vendor of family empowerment tools, reports almost six million visitors to their site since last July. The National Center for Missing and Exploited Children, another of our partners, receives 2.3 million hits per day, but cannot distinguish between those

seeking information about child safety online and those looking at images of missing children. AOL has two pages, Neighborhood Watch and Parental Controls, that deal with child safety and include the GetNetWise link. Neighborhood Watch has averaged about 472,000 visitors per month, while Parental Controls has averaged about 2,084,000 visitors. Though not comparably measured, we feel that we have evidence of abundant interest in the problem of child safety online, and the solution of family empowerment.

- **User Satisfaction**

We do not yet have an online satisfaction survey for users, but we do provide a link which enables users to contact either the Webmaster or the GetNetWise director with questions and concerns. To date, our correspondents have expressed little dissatisfaction with GetNetWise, but many have used the link to comment on objectionable materials that they have found online.

One of our partners, Net Nanny, has noted that GetNetWise has been extremely well received by attendees of "Internet and Your Child." IYC is a training program on Internet safety for parents, teachers, and law enforcement officers. Net Nanny, a founding member, core curriculum developer, and master trainer for the IYC program, passed on this comment:

> We have heard tons of great feedback from Leanne Shirey, a vice detective with the Seattle Police Department and the founder of the "Internet and Your Child" program. IYC students have been very impressed with GetNetWise and consider it to be one of the more useful resources for additional information offered during the training and afterward when they are home searching for ways to control their kids' online activities. They found the resource informative (especially the tools section), easy to use and potentially very helpful in the event that their children run into trouble online.

What are the next steps for GetNetWise?

- **Content enhancement**

Because interactivity is considered the most dangerous aspect of the online world, we will soon be adding new privacy tools to help prevent children from inadvertently providing personal and potentially dangerous information to strangers. We will also be adding new tools that will allow parents to intervene if their children are subjected to threatening or hateful materials or language, on a Web site, or in a chat room or instant message.

We plan to collect and tabulate user satisfaction data by introducing a "Talk Back" feature. We will be soliciting the opinions of users about the effectiveness of the tools they've selected for use, and the response they get when they report hate speech to authorities via our links. We'll also ask if they've identified any new tools which we've not included in our directory. Our Web master will regularly read the comments to assess needs for changes to the site.

Other surveys will focus on parents, caregivers, and children and youth who use the Internet, including those currently using GetNetWise. Our goal is to learn how best to protect children and youth within the framework of rapid technological change. The surveys and focus groups will help us refine our understanding of what's working, and determine what we can improve.

- **Increased reach and awareness**

GetNetWise will undertake several initiatives to broaden our reach and make our site available to more families as they go online. The development and launch of a Spanish-language version of GetNetWise will make our resources and tools accessible to more than 33 million Spanish-speaking Americans. And our focus on creating partnerships with the smaller ISPs will bring us closer to our goal of being one click away from 95% of the Internet users. Our penetration of the 6000 small to

medium size ISPs remains low, and we will need to recruit a significant number of new partners among them.

As we work to make the tools and resources of GetNetWise more readily accessible, we are also cognizant of the need to raise public awareness of the issue of child online safety and family empowerment.

This summer, at its first year anniversary, GetNetWise plans to re-launch at an event on Capitol Hill. The event will present us with a stage from which to celebrate accomplishments and to preview the exciting developments planned for year two. It will also give us an opportunity to rekindle the interest of the media and key public officials as we begin our second year. As before, we expect that an aggressive media campaign will bring our message to policy makers and millions of American homes, via broadcast, print, and online media. After the re-launch, we want to continue earning media attention as credible spokespersons for family empowerment and online safety.

We will also be paying more attention to non-Internet-using parents. With the help of our partners, we will be employing the familiar and comfortable medium of print to reach those parents who lack the knowledge or means to get our materials online. Parents' guides, teachers' guides, and public officials' guides can all be part of the mix which lets "non-online" parents know that they, too, have both the responsibility and the wherewithal to help their children safely explore the online world. Articles placed in local or community newspapers will continue the outreach to these families.

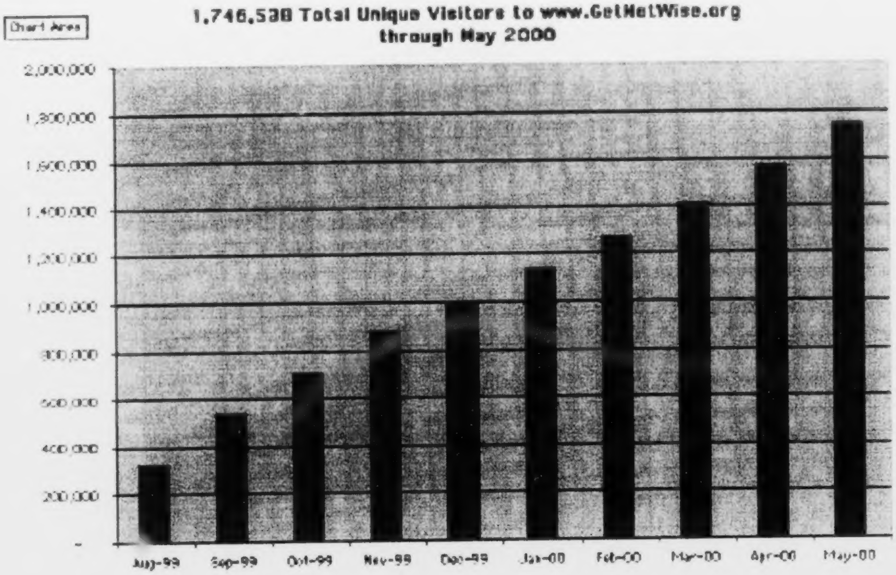
One medium which we will not be using to reach parents is unsolicited e-mail. Those who use the Internet would not be receptive to this form of message delivery, and those who are not yet online would be overlooked.

Other elements in our national communications plan include a Public Service Announcement (PSA) campaign possibly in conjunction with the Advertising

Council, and a strategic earned media campaign addressed to publications, reporters, and editors covering technology, education, consumer affairs, and women's, children's, and family issues. We will develop reporting mechanisms that will allow us to monitor and assess the results of awareness programs.

Summary

In the past ten months, the Internet community and its public interest partners have made a promising start towards providing parents with the resources they need to guide their children through the sometimes risky world of the Internet. Over 90% of Internet users have one-click access to GetNetWise, a Web site that links parents with sound advice, information, references, and access to over 110 tools. Parents can select the appropriate means to help their children safely enjoy the educational and entertaining bounty of the World Wide Web, consistent with their own values and the age and needs of their children. Web site development proceeds, with new tools and links planned for upcoming release. As public education remains a key challenge the partnership will continue to raise public awareness that engaged and empowered parents are a child's best defense against unwanted and unwelcome online content and encounters.



BEST COPY AVAILABLE

David Eisner
Vice President, Corporate Relations
America Online, Inc.

David Eisner is the Vice-President of Corporate Relations at America Online. He has helped manage the company's corporate communications since 1995, first as a consultant and since May, 1997, in his current position. Reporting to Chief Communications Officer Kathy Bushkin, David oversees AOL's executive communications and public policy communications as well as corporate events, internal and community relations and the AOL Foundation.

Before joining AOL full-time, David served as Senior Vice President at Fleishman-Hillard International Communications, in their Washington, DC office. He led the telecommunications practice at Fleishman-Hillard from 1993 until joining the AOL team in 1997. He specialized in corporate reputation and public affairs issues management.

From 1990 to 1993, David worked as the Director of Communications for the Legal Service Corporation, a quasi-federal, Congressionally supported agency, and one of the largest public non-profit institutions in the United States. David began his career on Capitol Hill as press secretary for several Members of Congress from 1985-1990. He graduated from Stanford University with a BA in creative writing.

COPA Commission Hearing

June 8, 2000

Introduction

It is a pleasure for us to be here before the COPA Commission and to discuss GetNetWise a comprehensive toolbox of resources for parents that is widely distributed online. GetNetWise is a direct response to the serious need to protect children online from unwanted and inappropriate content or contacts. On the Internet, GetNetWise is designed to be easy to use and easily accessible "one click away." That powerful click is the response to a challenge to the Internet industry to help families keep their children safe online while affording them the opportunity to take full advantage of the learning and recreational potential of this global medium.

GetNetWise is a direct response to the Internet medium – a world wide network, without borders or centralized points of control. The Internet is not physically contained within the jurisdiction of a locality, state, or nation, nor subject to the laws of any one nation. It is an open medium, in which people all over the world determine the course of their own online activities, viewing and creating content. A click on a link can send content racing from a computer half way around the world, jumping oceans as easily as city lines.

Who exercises control of this content? No one, and everyone. No one has the means to control, or limit, or legislate what the world will put on the World Wide Web. But everyone has the means to limit what comes in to his or her own computer. The power to control content lies with the end users. And when the end users are children, control should lie with parents or caregivers.

Parents are finding that with one click of a mouse, they can gain access to information needed to help ensure that the Internet is an educational and entertaining world for their children to explore, safe from unwanted and inappropriate content or contacts. That

powerful click is the response to a challenge to the Internet industry, to help families keep their children safe online.

The challenge embraced by GetNetWise is two-fold: first, to assemble information about the use and deployment of online empowerment tools into a common, easy-to-use resource for parents, and second, to ensure that the resource has the widest distribution possible, so that it is essentially one click away.

Both Congress and the Administration worked with Internet industry leaders and well-known family groups in the 1997 Internet Online Summit and the 1998 America Links Up campaign to address children's safety online. Since then, the Internet industry has focused on creating a collection of resources that would be accessible from the major entry points to the Internet and that would provide families with information on how to guide their children online. The Child Online Protection Act (COPA) asked whether providing one click access to such a common resource for parents was feasible. Before the COPA Commission even convened to examine this question, a partnership of Internet companies and public interest groups came together with the goal to create just such a resource.

The partnership, which includes AOL, AT&T, Alta Vista, Bell Atlantic, Bell South, Cyber Patrol, Dell, Disney Online, EarthLink, Excite@Home, IBM, Lycos, WorldCom, Microsoft, Net Nanny, Network Solutions, Prodigy, Road Runner, Surf Watch Software, Yahoo!, Zeeks, the American Library Association, Association of American Publishers, Center for Democracy and Technology, Center for Media Education, The Children's Partnership, Commercial Internet eXchange, Cyberangels, Enough is Enough, Internet Alliance, Internet Content Rating Association, National Center for Missing and Exploited Children, NetFamilyNews, People for the American Way, and the US Chamber of Commerce, believes that this goal was reached when GetNetWise was launched in July, 1999, demonstrating that one-click away access was not just feasible, but operational. For the past ten months, it has been helping parents keep children safe by giving them the means to guide their children's online activities. Parents need only to access the child

safety page on their Internet Service Provider (ISP), Online Service Provider (OSP), or portal site, and they will be but one click away from the resources that the partnership has made available on GetNetWise.

Why GetNetWise?

GetNetWise offers parents and caregivers the most effective technological and legal means by which they can protect their children from unwanted and age-inappropriate content on the Internet.

Through GetNetWise, a public service sponsored by Internet companies and public interest organizations, families can find the means to exercise that power in their own homes, making the Internet a safe and valuable resource for their kids. GetNetWise is more than a Web site. It represents a commitment to child safety from ISPs, OSPs, and portals. These companies, which serve as gateways to the Internet for over 90% of Internet users in the country, have given parents one-click access from their sites to family-friendly information and tools for online safety.

As the Internet grows, it is augmenting or supplanting other media such as newspapers, television and radio. Parents and educators realize that denying children access to the Web, and all the benefits that access confers, is a great risk—though certainly not the only one. As children plunge into an array of educational, entertaining, and wholesomely engaging resources, they may come upon other, objectionable material. At GetNetWise, we know that the best way to have kids be safe users is to empower their parents to guide their Internet explorations and help them make good choices, based on their family's values and the child's ages and maturity.

Establishing guidelines and standards can be a challenge for parents. Often parents are less familiar with Internet technology than their children. While parents may make little or no use of the Internet, many children are using it in school or in the library, and are even becoming Web authors as their own class projects are posted to school Web pages.

Often they use the Internet at home without adult supervision. Parents who want to understand the alternatives available to them to help their children stay safe online find GetNetWise to be a valuable resource.

What makes GetNetWise so useful? First, accessibility: Over 90% of online users have one-click access through their ISP, OSP, or popular portal sites, via a button or link which connects them directly to GetNetWise resources. Second, we help parents understand the nature of the risks that their children face online, and suggest actions they can take in response. Third, we offer a list of recommended sites appropriate for children, and finally, we give parents access to tools which will help them make their children's online experience safe and enriching. GetNetWise is regularly updated so parents can be assured that the information they are getting is current.

What kind of helpful information will parents find through GetNetWise?

GetNetWise provides four types of information:

- **Online Safety Guide**

The Safety Guide provides information about the potential safety and privacy risks to children online. In a frank but friendly tone, the guide helps parents learn about the kind of material available on the Internet, and what issues merit their concern. It explains that the primary appeal of the Internet, interactivity, is also the attribute which creates the greatest risk. But what's new to parents may already be second nature to children; parents may find they're learning things their children already know.

Because one solution doesn't fit all children or all families, the safety guide addresses the needs of children by age/maturity level, and offers general tips for children, teens, and families. It also covers specific risks, and offers strategies to deal with each. In some situations, technology may offer parents a way to solve a particular problem;

when that is the case, a link can take parents directly to Tools for Families, where they can learn about the tool and what it can do for them.

- **Tools for Families**

The tools section provides a comprehensive directory of over 110 technology tools that families can use to filter, block or monitor access to inappropriate content, such as violent or sexually explicit materials. The directory also includes tools which filter, block, or monitor outgoing materials, such as e-mails or chat rooms where children might post information. Parents can learn about the different ways that these tools work, and the standards that they apply, to determine what tools will work best for their family. These tools can be changed or altered as kids grow up and can be personalized to each computer and each user in the house. A searchable database allows parents to identify their needs and see a list of appropriate tools. Links to the tool providers allow parents to download the latest versions.

Because we want parents to have as much information as possible about available technology, we add new tools to the GetNetWise database when they are made available. We keep the database current by actively looking for new tools, and we provide an online request that developers can use to tell us about their new family empowerment software. The criteria for inclusion on the tools directory are posted, and of course, there is no charge to the software companies for the listings. Currently, there are more than 110 tools listed in the directory.

Interestingly, one of the frequently viewed tools is not a technological solution at all, but a sample contract or agreement, which sets out in simple language the rules that a child agrees to follow when going online. The child pledges to follow the rules that minimize his or her risk, and to keep parents or caregivers informed if anything untoward happens. Links to other such contracts are also provided.

- **Reporting Trouble Online**

For many parents, the first indication that they need to be involved in their child's online activities comes when they see that a child has accessed inappropriate or objectionable materials. In a panic because their child has been exposed to pornography or other pernicious content, they may assume that a law has been broken. This section of GetNetWise helps parents understand the difference between material that is illegal and material that is inappropriate for their child, and between what is dangerous and what is merely annoying.

More important, it provides information on what steps to take in response to various situations, from calling law enforcement if a child's safety is immediately threatened to reporting sites which include illegal material. Should the situation warrant a call to law enforcement, links are provided to state police and to federal law enforcement agencies. These agencies can provide comprehensive advice about dealing with online problems. Additionally, there are links and/or phone numbers for child advocacy organizations involved with various threats to children, in both the online and physical worlds.

- **Web Sites for Kids**

Parents often look to "Kid-Safe" Web sites to provide a safe and enjoyable online haven for their children. Our list includes current sites that have been developed or recommended by our partners or by other family-oriented non-profit groups and child development experts.

Parents need options based on their values and the needs of their children. Some may choose to use tools which will limit their children's viewing to sites such as these or other kid-oriented sites. But, as they learn when they read about blocking and filtering technology, they may be restricting their children's access to valuable and appropriate information. A young girl entering puberty, for example, may seek information about the changes her body is undergoing, but find that any mention of reproductive organs has been screened from the content she is permitted to see. As children grow up, their

information needs change, and GetNetWise can give their parents the resources they need to make decisions about their child's online access.

How have parents been made aware of GetNetWise?

The July, 1999, launch of GetNetWise generated widespread coverage, reaching millions of American homes through television, radio and print media. Attendance of key policymakers, corporate executives, and other well-known supporters at the launch ensured coverage in all top ten television markets, as well as 50 smaller markets. C-Span coverage and rebroadcasts, video news releases and repackaged news releases continued to enlarge the number of viewers reached. Print coverage by the *New York Times, Washington Post, USA Today, Christian Science Monitor, Los Angeles Times*, and the wire services extended the story, as did coverage by online zines such as C/Net, Newsbytes, PCWeek Online, ZDNet, and others.

Since the launch, GetNetWise and its partners have continued to earn media coverage in connection with safety for children online. We have promoted the site in a variety of ways, including banner ads and buttons displayed on the Web, bookmarks distributed at libraries, print brochures distributed at trade shows for educators, advertisements on bags of Wise Potato Chips, and promotional video screens displayed at 7-11 Stores. Information about GetNetWise is included in briefings of policymakers and public officials at federal, state, and local levels.

Partners and supporters provide one-click linkage to the GetNetWise site (or their own functional equivalent site) from their own Web sites, and they often promote the site in other ways. For example, AT&T gives the logo a prominent position, has included the site in an online shopping guide for consumers, and listed it as a resource on their "Parents" page. Lycos distributes GetNetWise capability brochures at all events attended by Lycos Zone, including trade shows pertinent to children and educators, and information about GetNetWise is included in Lycos Zone press kits at shows and press events. Microsoft runs banner ads on MSN, and includes information about GetNetWise

in appropriate press announcements and online feature stories. The National Center for Missing and Exploited Children and Net Nanny introduce and promote GetNetWise at classes conducted for law enforcement, parents, and teachers.

Interest in online safety and potential solutions for parents has filtered from the technology world into the mainstream, increasing the visibility of GetNetWise. No longer just the purview of technology writers, online safety is now addressed by journalists who cover education, family issues, children, and consumer affairs. References to GetNetWise have recently appeared in articles about privacy, as well as in an article about how parents are finally taking cues from their children and using the Internet to trade parenting tips. A recent episode of CBS Television's "Touched by an Angel" dealt with online safety, and referred viewers and Web site visitors to Enough is Enough, the National Center for Missing and Exploited Children, and Safekids.com, all GetNetWise advisors.

How are parents responding to GetNetWise?

- **Traffic**

  During the first ten months since GetNetWise came online, it provided 1,746,538 online users access to this resource, representing more than 12 million hits. Also, these numbers do not include page views by those partners, particularly Yahoo!, that provide their own version of GetNetWise resources tailored for their audiences

  Information from our partners indicates that online child safety resources generate a great deal of traffic. But understandably, not all of our partners tally the visits to their child safety pages, and those who do may count them differently. Some have numerous features bundled into their child safety pages, which makes extraction for purposes of assessing their link to GetNetWise impossible. Net Nanny, for example, a vendor of family empowerment tools, reports almost six million visitors to their site since last July. The National Center for Missing and Exploited Children, another of our partners, receives 2.3 million hits per day, but cannot distinguish between those

seeking information about child safety online and those looking at images of missing children. AOL has two pages, Neighborhood Watch and Parental Controls, that deal with child safety and include the GetNetWise link. Neighborhood Watch has averaged about 472,000 visitors per month, while Parental Controls has averaged about 2,084,000 visitors. Though not comparably measured, we feel that we have evidence of abundant interest in the problem of child safety online, and the solution of family empowerment.

- **User Satisfaction**

We do not yet have an online satisfaction survey for users, but we do provide a link which enables users to contact either the Webmaster or the GetNetWise director with questions and concerns. To date, our correspondents have expressed little dissatisfaction with GetNetWise, but many have used the link to comment on objectionable materials that they have found online.

One of our partners, Net Nanny, has noted that GetNetWise has been extremely well received by attendees of "Internet and Your Child." IYC is a training program on Internet safety for parents, teachers, and law enforcement officers. Net Nanny, a founding member, core curriculum developer, and master trainer for the IYC program, passed on this comment:

> We have heard tons of great feedback from Leanne Shirey, a vice detective with the Seattle Police Department and the founder of the "Internet and Your Child" program. IYC students have been very impressed with GetNetWise and consider it to be one of the more useful resources for additional information offered during the training and afterward when they are home searching for ways to control their kids' online activities. They found the resource informative (especially the tools section), easy to use and potentially very helpful in the event that their children run into trouble online.

What are the next steps for GetNetWise?

- **Content enhancement**

Because interactivity is considered the most dangerous aspect of the online world, we will soon be adding new privacy tools to help prevent children from inadvertently providing personal and potentially dangerous information to strangers. We will also be adding new tools that will allow parents to intervene if their children are subjected to threatening or hateful materials or language, on a Web site, or in a chat room or instant message.

We plan to collect and tabulate user satisfaction data by introducing a "Talk Back" feature. We will be soliciting the opinions of users about the effectiveness of the tools they've selected for use, and the response they get when they report hate speech to authorities via our links. We'll also ask if they've identified any new tools which we've not included in our directory. Our Web master will regularly read the comments to assess needs for changes to the site.

Other surveys will focus on parents, caregivers, and children and youth who use the Internet, including those currently using GetNetWise. Our goal is to learn how best to protect children and youth within the framework of rapid technological change. The surveys and focus groups will help us refine our understanding of what's working, and determine what we can improve.

- **Increased reach and awareness**

GetNetWise will undertake several initiatives to broaden our reach and make our site available to more families as they go online. The development and launch of a Spanish-language version of GetNetWise will make our resources and tools accessible to more than 33 million Spanish-speaking Americans. And our focus on creating partnerships with the smaller ISPs will bring us closer to our goal of being one click away from 95% of the Internet users. Our penetration of the 6000 small to

medium size ISPs remains low, and we will need to recruit a significant number of new partners among them.

As we work to make the tools and resources of GetNetWise more readily accessible, we are also cognizant of the need to raise public awareness of the issue of child online safety and family empowerment.

This summer, at its first year anniversary, GetNetWise plans to re-launch at an event on Capitol Hill. The event will present us with a stage from which to celebrate accomplishments and to preview the exciting developments planned for year two. It will also give us an opportunity to rekindle the interest of the media and key public officials as we begin our second year. As before, we expect that an aggressive media campaign will bring our message to policy makers and millions of American homes, via broadcast, print, and online media. After the re-launch, we want to continue earning media attention as credible spokespersons for family empowerment and online safety.

We will also be paying more attention to non-Internet-using parents. With the help of our partners, we will be employing the familiar and comfortable medium of print to reach those parents who lack the knowledge or means to get our materials online. Parents' guides, teachers' guides, and public officials' guides can all be part of the mix which lets "non-online" parents know that they, too, have both the responsibility and the wherewithal to help their children safely explore the online world. Articles placed in local or community newspapers will continue the outreach to these families.

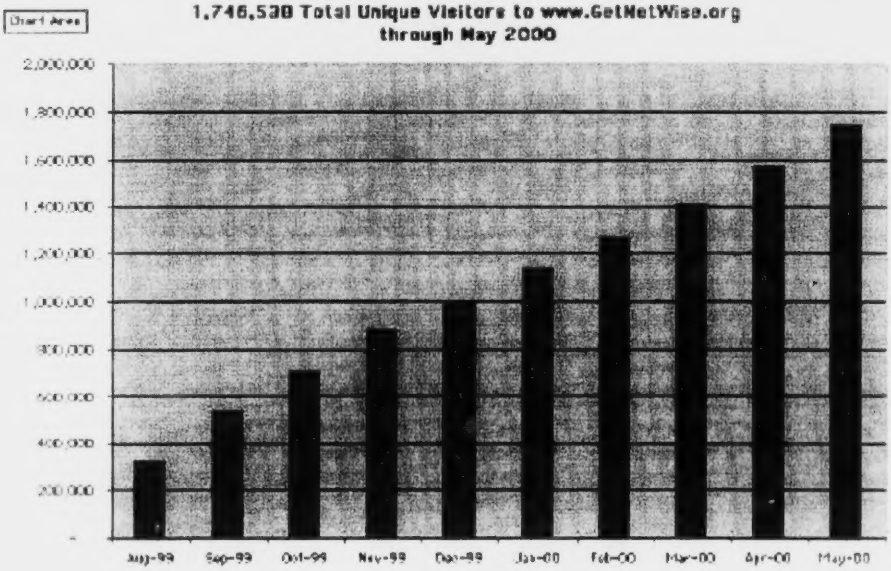
One medium which we will not be using to reach parents is unsolicited e-mail. Those who use the Internet would not be receptive to this form of message delivery, and those who are not yet online would be overlooked.

Other elements in our national communications plan include a Public Service Announcement (PSA) campaign possibly in conjunction with the Advertising

Council, and a strategic earned media campaign addressed to publications, reporters, and editors covering technology, education, consumer affairs, and women's, children's, and family issues. We will develop reporting mechanisms that will allow us to monitor and assess the results of awareness programs.

Summary

In the past ten months, the Internet community and its public interest partners have made a promising start towards providing parents with the resources they need to guide their children through the sometimes risky world of the Internet. Over 90% of Internet users have one-click access to GetNetWise, a Web site that links parents with sound advice, information, references, and access to over 110 tools. Parents can select the appropriate means to help their children safely enjoy the educational and entertaining bounty of the World Wide Web, consistent with their own values and the age and needs of their children. Web site development proceeds, with new tools and links planned for upcoming release. As public education remains a key challenge the partnership will continue to raise public awareness that engaged and empowered parents are a child's best defense against unwanted and unwelcome online content and encounters.



1,746,538 Total Unique Visitors to www.GetNetWise.org through May 2000

Marilyn S. Cade, AT&T

Director, Internet and E-Commerce, Law and Government Affairs
1120 20th Street, N.W., Suite 1000, Washington, D.C. 20036
P (202) 457-2106 C (202) 255-7348
mcade@att.com

Marilyn Cade is responsible for Internet and E-Commerce advocacy and policy issues, including intellectual property, Internet security, privacy, and content regulation, domestically and internationally. She also directs AT&T's advocacy activity on these issues with ad hoc organizations, professional organizations and associations. Her focus is the nexus of technology and public policy and implications for the Internet, online services, and electronic commerce.

In addition to advocacy and technology policy, her career with AT&T has included a number of management positions with AT&T's business units in sales, marketing, business operations and strategy. Prior to joining AT&T, she spent 9 years in a variety of non-profit organizations and state government positions.

AT&T is the world's premier voice and data communications company, serving more than 80 million customers, including consumers, businesses and governments. With annual revenues of more than $52 billion and some 140,000 employees, AT&T provides services to countries and territories around the world. The company is a leading provider of communications and IP services to businesses and is the nation's largest direct Internet Service Provider to consumers. AT&T's businesses are backed by the research and development capabilities of AT&T Labs, which is working to create the information services and communications networks of tomorrow.

COPA Commission Hearing

June 8, 2000

Introduction

It is a pleasure for us to be here before the COPA Commission and to discuss GetNetWise a comprehensive toolbox of resources for parents that is widely distributed online. GetNetWise is a direct response to the serious need to protect children online from unwanted and inappropriate content or contacts. On the Internet, GetNetWise is designed to be easy to use and easily accessible "one click away." That powerful click is the response to a challenge to the Internet industry to help families keep their children safe online while affording them the opportunity to take full advantage of the learning and recreational potential of this global medium.

GetNetWise is a direct response to the Internet medium – a world wide network, without borders or centralized points of control. The Internet is not physically contained within the jurisdiction of a locality, state, or nation, nor subject to the laws of any one nation. It is an open medium, in which people all over the world determine the course of their own online activities, viewing and creating content. A click on a link can send content racing from a computer half way around the world, jumping oceans as easily as city lines.

Who exercises control of this content? No one, and everyone. No one has the means to control, or limit, or legislate what the world will put on the World Wide Web. But everyone has the means to limit what comes in to his or her own computer. The power to control content lies with the end users. And when the end users are children, control should lie with parents or caregivers.

Parents are finding that with one click of a mouse, they can gain access to information needed to help ensure that the Internet is an educational and entertaining world for their children to explore, safe from unwanted and inappropriate content or contacts. That

powerful click is the response to a challenge to the Internet industry, to help families keep their children safe online.

The challenge embraced by GetNetWise is two-fold: first, to assemble information about the use and deployment of online empowerment tools into a common, easy-to-use resource for parents, and second, to ensure that the resource has the widest distribution possible, so that it is essentially one click away.

Both Congress and the Administration worked with Internet industry leaders and well-known family groups in the 1997 Internet Online Summit and the 1998 America Links Up campaign to address children's safety online. Since then, the Internet industry has focused on creating a collection of resources that would be accessible from the major entry points to the Internet and that would provide families with information on how to guide their children online. The Child Online Protection Act (COPA) asked whether providing one click access to such a common resource for parents was feasible. Before the COPA Commission even convened to examine this question, a partnership of Internet companies and public interest groups came together with the goal to create just such a resource.

The partnership, which includes AOL, AT&T, Alta Vista, Bell Atlantic, Bell South, Cyber Patrol, Dell, Disney Online, EarthLink, Excite@Home, IBM, Lycos, WorldCom, Microsoft, Net Nanny, Network Solutions, Prodigy, Road Runner, Surf Watch Software, Yahoo!, Zeeks, the American Library Association, Association of American Publishers, Center for Democracy and Technology, Center for Media Education, The Children's Partnership, Commercial Internet eXchange, Cyberangels, Enough is Enough, Internet Alliance, Internet Content Rating Association, National Center for Missing and Exploited Children, NetFamilyNews, People for the American Way, and the US Chamber of Commerce, believes that this goal was reached when GetNetWise was launched in July, 1999, demonstrating that one-click away access was not just feasible, but operational. For the past ten months, it has been helping parents keep children safe by giving them the means to guide their children's online activities. Parents need only to access the child

safety page on their Internet Service Provider (ISP), Online Service Provider (OSP), or portal site, and they will be but one click away from the resources that the partnership has made available on GetNetWise.

Why GetNetWise?

GetNetWise offers parents and caregivers the most effective technological and legal means by which they can protect their children from unwanted and age-inappropriate content on the Internet.

Through GetNetWise, a public service sponsored by Internet companies and public interest organizations, families can find the means to exercise that power in their own homes, making the Internet a safe and valuable resource for their kids. GetNetWise is more than a Web site. It represents a commitment to child safety from ISPs, OSPs, and portals. These companies, which serve as gateways to the Internet for over 90% of Internet users in the country, have given parents one-click access from their sites to family-friendly information and tools for online safety.

As the Internet grows, it is augmenting or supplanting other media such as newspapers, television and radio. Parents and educators realize that denying children access to the Web, and all the benefits that access confers, is a great risk—though certainly not the only one. As children plunge into an array of educational, entertaining, and wholesomely engaging resources, they may come upon other, objectionable material. At GetNetWise, we know that the best way to have kids be safe users is to empower their parents to guide their Internet explorations and help them make good choices, based on their family's values and the child's ages and maturity.

Establishing guidelines and standards can be a challenge for parents. Often parents are less familiar with Internet technology than their children. While parents may make little or no use of the Internet, many children are using it in school or in the library, and are even becoming Web authors as their own class projects are posted to school Web pages.

Often they use the Internet at home without adult supervision. Parents who want to understand the alternatives available to them to help their children stay safe online find GetNetWise to be a valuable resource.

What makes GetNetWise so useful? First, accessibility: Over 90% of online users have one-click access through their ISP, OSP, or popular portal sites, via a button or link which connects them directly to GetNetWise resources. Second, we help parents understand the nature of the risks that their children face online, and suggest actions they can take in response. Third, we offer a list of recommended sites appropriate for children, and finally, we give parents access to tools which will help them make their children's online experience safe and enriching. GetNetWise is regularly updated so parents can be assured that the information they are getting is current.

What kind of helpful information will parents find through GetNetWise?

GetNetWise provides four types of information:

- **Online Safety Guide**

  The Safety Guide provides information about the potential safety and privacy risks to children online. In a frank but friendly tone, the guide helps parents learn about the kind of material available on the Internet, and what issues merit their concern. It explains that the primary appeal of the Internet, interactivity, is also the attribute which creates the greatest risk. But what's new to parents may already be second nature to children; parents may find they're learning things their children already know.

  Because one solution doesn't fit all children or all families, the safety guide addresses the needs of children by age/maturity level, and offers general tips for children, teens, and families. It also covers specific risks, and offers strategies to deal with each. In some situations, technology may offer parents a way to solve a particular problem;

when that is the case, a link can take parents directly to Tools for Families, where they can learn about the tool and what it can do for them.

- **Tools for Families**

The tools section provides a comprehensive directory of over 110 technology tools that families can use to filter, block or monitor access to inappropriate content, such as violent or sexually explicit materials. The directory also includes tools which filter, block, or monitor outgoing materials, such as e-mails or chat rooms where children might post information. Parents can learn about the different ways that these tools work, and the standards that they apply, to determine what tools will work best for their family. These tools can be changed or altered as kids grow up and can be personalized to each computer and each user in the house. A searchable database allows parents to identify their needs and see a list of appropriate tools. Links to the tool providers allow parents to download the latest versions.

Because we want parents to have as much information as possible about available technology, we add new tools to the GetNetWise database when they are made available. We keep the database current by actively looking for new tools, and we provide an online request that developers can use to tell us about their new family empowerment software. The criteria for inclusion on the tools directory are posted, and of course, there is no charge to the software companies for the listings. Currently, there are more than 110 tools listed in the directory.

Interestingly, one of the frequently viewed tools is not a technological solution at all, but a sample contract or agreement, which sets out in simple language the rules that a child agrees to follow when going online. The child pledges to follow the rules that minimize his or her risk, and to keep parents or caregivers informed if anything untoward happens. Links to other such contracts are also provided.

- **Reporting Trouble Online**

For many parents, the first indication that they need to be involved in their child's online activities comes when they see that a child has accessed inappropriate or objectionable materials. In a panic because their child has been exposed to pornography or other pernicious content, they may assume that a law has been broken. This section of GetNetWise helps parents understand the difference between material that is illegal and material that is inappropriate for their child, and between what is dangerous and what is merely annoying.

More important, it provides information on what steps to take in response to various situations, from calling law enforcement if a child's safety is immediately threatened to reporting sites which include illegal material. Should the situation warrant a call to law enforcement, links are provided to state police and to federal law enforcement agencies. These agencies can provide comprehensive advice about dealing with online problems. Additionally, there are links and/or phone numbers for child advocacy organizations involved with various threats to children, in both the online and physical worlds.

- **Web Sites for Kids**

Parents often look to "Kid-Safe" Web sites to provide a safe and enjoyable online haven for their children. Our list includes current sites that have been developed or recommended by our partners or by other family-oriented non-profit groups and child development experts.

Parents need options based on their values and the needs of their children. Some may choose to use tools which will limit their children's viewing to sites such as these or other kid-oriented sites. But, as they learn when they read about blocking and filtering technology, they may be restricting their children's access to valuable and appropriate information. A young girl entering puberty, for example, may seek information about the changes her body is undergoing, but find that any mention of reproductive organs has been screened from the content she is permitted to see. As children grow up, their

information needs change, and GetNetWise can give their parents the resources they need to make decisions about their child's online access.

How have parents been made aware of GetNetWise?

The July, 1999, launch of GetNetWise generated widespread coverage, reaching millions of American homes through television, radio and print media. Attendance of key policymakers, corporate executives, and other well-known supporters at the launch ensured coverage in all top ten television markets, as well as 50 smaller markets. C-Span coverage and rebroadcasts, video news releases and repackaged news releases continued to enlarge the number of viewers reached. Print coverage by the *New York Times, Washington Post, USA Today, Christian Science Monitor, Los Angeles Times*, and the wire services extended the story, as did coverage by online zines such as C/Net, Newsbytes, PCWeek Online, ZDNet, and others.

Since the launch, GetNetWise and its partners have continued to earn media coverage in connection with safety for children online. We have promoted the site in a variety of ways, including banner ads and buttons displayed on the Web, bookmarks distributed at libraries, print brochures distributed at trade shows for educators, advertisements on bags of Wise Potato Chips, and promotional video screens displayed at 7-11 Stores. Information about GetNetWise is included in briefings of policymakers and public officials at federal, state, and local levels.

Partners and supporters provide one-click linkage to the GetNetWise site (or their own functional equivalent site) from their own Web sites, and they often promote the site in other ways. For example, AT&T gives the logo a prominent position, has included the site in an online shopping guide for consumers, and listed it as a resource on their "Parents" page. Lycos distributes GetNetWise capability brochures at all events attended by Lycos Zone, including trade shows pertinent to children and educators, and information about GetNetWise is included in Lycos Zone press kits at shows and press events. Microsoft runs banner ads on MSN, and includes information about GetNetWise

in appropriate press announcements and online feature stories. The National Center for Missing and Exploited Children and Net Nanny introduce and promote GetNetWise at classes conducted for law enforcement, parents, and teachers.

Interest in online safety and potential solutions for parents has filtered from the technology world into the mainstream, increasing the visibility of GetNetWise. No longer just the purview of technology writers, online safety is now addressed by journalists who cover education, family issues, children, and consumer affairs. References to GetNetWise have recently appeared in articles about privacy, as well as in an article about how parents are finally taking cues from their children and using the Internet to trade parenting tips. A recent episode of CBS Television's "Touched by an Angel" dealt with online safety, and referred viewers and Web site visitors to Enough is Enough, the National Center for Missing and Exploited Children, and Safekids.com, all GetNetWise advisors.

How are parents responding to GetNetWise?

- **Traffic**

During the first ten months since GetNetWise came online, it provided 1,746,538 online users access to this resource, representing more than 12 million hits. Also, these numbers do not include page views by those partners, particularly Yahoo!, that provide their own version of GetNetWise resources tailored for their audiences.

Information from our partners indicates that online child safety resources generate a great deal of traffic. But understandably, not all of our partners tally the visits to their child safety pages, and those who do may count them differently. Some have numerous features bundled into their child safety pages, which makes extraction for purposes of assessing their link to GetNetWise impossible. Net Nanny, for example, a vendor of family empowerment tools, reports almost six million visitors to their site since last July. The National Center for Missing and Exploited Children, another of our partners, receives 2.3 million hits per day, but cannot distinguish between those

seeking information about child safety online and those looking at images of missing children. AOL has two pages, Neighborhood Watch and Parental Controls, that deal with child safety and include the GetNetWise link. Neighborhood Watch has averaged about 472,000 visitors per month, while Parental Controls has averaged about 2,084,000 visitors. Though not comparably measured, we feel that we have evidence of abundant interest in the problem of child safety online, and the solution of family empowerment.

- **User Satisfaction**

We do not yet have an online satisfaction survey for users, but we do provide a link which enables users to contact either the Webmaster or the GetNetWise director with questions and concerns. To date, our correspondents have expressed little dissatisfaction with GetNetWise, but many have used the link to comment on objectionable materials that they have found online.

One of our partners, Net Nanny, has noted that GetNetWise has been extremely well received by attendees of "Internet and Your Child." IYC is a training program on Internet safety for parents, teachers, and law enforcement officers. Net Nanny, a founding member, core curriculum developer, and master trainer for the IYC program, passed on this comment:

> We have heard tons of great feedback from Leanne Shirey, a vice detective with the Seattle Police Department and the founder of the "Internet and Your Child" program. IYC students have been very impressed with GetNetWise and consider it to be one of the more useful resources for additional information offered during the training and afterward when they are home searching for ways to control their kids' online activities. They found the resource informative (especially the tools section), easy to use and potentially very helpful in the event that their children run into trouble online.

What are the next steps for GetNetWise?

- **Content enhancement**

Because interactivity is considered the most dangerous aspect of the online world, we will soon be adding new privacy tools to help prevent children from inadvertently providing personal and potentially dangerous information to strangers. We will also be adding new tools that will allow parents to intervene if their children are subjected to threatening or hateful materials or language, on a Web site, or in a chat room or instant message.

We plan to collect and tabulate user satisfaction data by introducing a "Talk Back" feature. We will be soliciting the opinions of users about the effectiveness of the tools they've selected for use, and the response they get when they report hate speech to authorities via our links. We'll also ask if they've identified any new tools which we've not included in our directory. Our Web master will regularly read the comments to assess needs for changes to the site.

Other surveys will focus on parents, caregivers, and children and youth who use the Internet, including those currently using GetNetWise. Our goal is to learn how best to protect children and youth within the framework of rapid technological change. The surveys and focus groups will help us refine our understanding of what's working, and determine what we can improve.

- **Increased reach and awareness**

GetNetWise will undertake several initiatives to broaden our reach and make our site available to more families as they go online. The development and launch of a Spanish-language version of GetNetWise will make our resources and tools accessible to more than 33 million Spanish-speaking Americans. And our focus on creating partnerships with the smaller ISPs will bring us closer to our goal of being one click away from 95% of the Internet users. Our penetration of the 6000 small to

medium size ISPs remains low, and we will need to recruit a significant number of new partners among them.

As we work to make the tools and resources of GetNetWise more readily accessible, we are also cognizant of the need to raise public awareness of the issue of child online safety and family empowerment.

This summer, at its first year anniversary, GetNetWise plans to re-launch at an event on Capitol Hill. The event will present us with a stage from which to celebrate accomplishments and to preview the exciting developments planned for year two. It will also give us an opportunity to rekindle the interest of the media and key public officials as we begin our second year. As before, we expect that an aggressive media campaign will bring our message to policy makers and millions of American homes, via broadcast, print, and online media. After the re-launch, we want to continue earning media attention as credible spokespersons for family empowerment and online safety.

We will also be paying more attention to non-Internet-using parents. With the help of our partners, we will be employing the familiar and comfortable medium of print to reach those parents who lack the knowledge or means to get our materials online. Parents' guides, teachers' guides, and public officials' guides can all be part of the mix which lets "non-online" parents know that they, too, have both the responsibility and the wherewithal to help their children safely explore the online world. Articles placed in local or community newspapers will continue the outreach to these families.

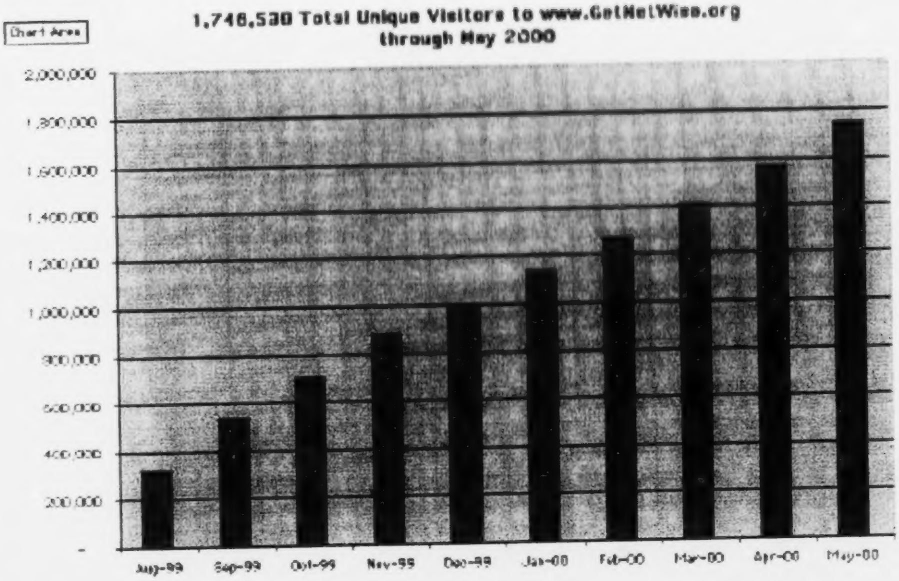
One medium which we will not be using to reach parents is unsolicited e-mail. Those who use the Internet would not be receptive to this form of message delivery, and those who are not yet online would be overlooked.

Other elements in our national communications plan include a Public Service Announcement (PSA) campaign possibly in conjunction with the Advertising

Council, and a strategic earned media campaign addressed to publications, reporters, and editors covering technology, education, consumer affairs, and women's, children's, and family issues. We will develop reporting mechanisms that will allow us to monitor and assess the results of awareness programs.

Summary

In the past ten months, the Internet community and its public interest partners have made a promising start towards providing parents with the resources they need to guide their children through the sometimes risky world of the Internet. Over 90% of Internet users have one-click access to GetNetWise, a Web site that links parents with sound advice, information, references, and access to over 110 tools. Parents can select the appropriate means to help their children safely enjoy the educational and entertaining bounty of the World Wide Web, consistent with their own values and the age and needs of their children. Web site development proceeds, with new tools and links planned for upcoming release. As public education remains a key challenge the partnership will continue to raise public awareness that engaged and empowered parents are a child's best defense against unwanted and unwelcome online content and encounters.



1,746,530 Total Unique Visitors to www.GetNetWise.org through May 2000

BEST COPY AVAILABLE

Parry Aftab is a cyberspace lawyer, author and child advocate. As the Executive Director of Cyberangels.org, the largest online safety and educational program in cyberspace which was awarded the President's Service Award in October, 1998, Ms Aftab works with law enforcement to police the Internet. Ms. Aftab is a worldwide leader in the area of online safety and parent and child Internet education. She also works closely with the FTC on online privacy and data collection practices. Ms. Aftab is on the advisory board for GetNetWise.

Ms. Aftab was recently appointed by UNESCO to head up its Innocence in Danger project for the U.S., to make sure that all children (regardless of wealth or ethnic background) can have safe access to the Internet (www.cyberangels.org/unescooverview.html). Its Wired Kids project, which launches in late March, 2000 (www.wiredkids.org) will be a collective effort of Internet leaders, educators, law enforcement, parents and librarians. It is designed to be a one-stop-shopping source for all matters related to children online, including online safety.

Her new book for parents and teachers on child online safety, The Parent's Guide to Protecting Your Children in Cyberspace, was be released by McGraw-Hill in January, 2000. The U.K. version of the book, written expressly for the parents and educators in the United Kingdom will be released in March, 2000. The book reviews the software and hardware options available to block, filter and monitor children's computer and Internet activity and provides practical solutions to parents' concerns about Internet safety. The book is, notwithstanding its subject matter, light and fun reading. Her first book, A Parents' Guide to the Internet...and how to protect your children in cyberspace, was released in January, 1998.

Ms. Aftab has helped design programs for parents and children teaching them how to use the Internet safely, including the P.I.E. Program (Parent Internet Education) for the Baltimore County School system. She is also an expert on filtering and blocking products. The FBI has even (unofficially) endorsed Ms. Aftab's work with online safety and her book.

Ms. Aftab also provides parent Internet education and online safety content for such diverse sites as Children's Television Workshop, Disney, Family.com, ABC's Children's First Foundation and MSNBC. Ms. Aftab was the Internet expert selected for the Littleton Town Meeting on MSNBC, hosted by Tom Brokaw and Jane Pauley, which featured Vice President Gore, among others. She was selected as one of the four key speakers at the White House Summit on Online Content, in Los Angeles, June 1998, and, as an expert in online privacy issues, was the keynote speaker at C.A.R.U's conference on children's online privacy in September, 1998. (C.A.R.U. is the advertising industry's joint project with the Better Business Bureau, and handles self-regulation matters.)

A free speech advocate, Ms. Aftab seeks to empower parents, not the censors. The book has been featured nationally in online and print publications, including U.S. News & World Report, Family Circle's Computing Made Easy, Newsweek, Smart Money Magazine, Family Circle, Good Housekeeping, The Sunday Times, Reader's Digest, Better Homes & Gardens and Home PC Magazine. As a result of her work online with children, Ms. Aftab was selected as a charter member of Children Television Workshop's Advisory Board, as well as appointed to The National Urban League's Technology Advisory Committee.

Parry Aftab has spoken to many groups, conducted an informal briefing for the U.S. Senate, been a key speaker at the White House Summit on Online Content and testified before leading legislative committees, all with the same message: The Internet is a wonderful resource for families, and once parents understand the online risks, they can use common sense (and perhaps some filtering tools) to help their children enjoy cyberspace safely.

Parry Aftab is admitted to practice in New York and New Jersey. She attended law school at NYU School of Law. She was Valedictorian of Hunter College (having completed her undergraduate degree in less than two years), where she was inducted into *Phi Beta Kappa*.

She can be reached at Parry@Aftab.com, or at her law firm: Aftab & Savitt, P.C. 22 Route 22 West Springfield, NJ 07081 (973) 467-3000 Fax- (973) 467-3051

TESTIMONY OF PARRY AFTAB, EXECUTIVE DIRECTOR OF CYBERANGELS

BEFORE THE COPA COMMISSION

JUNE 8, 2000

Cyberangels is the world's oldest and largest Internet safety, help and educational program. Formed in 1995 by Guardian Angels, in response to a call-in listener's request to Curtis Sliwa, ABC Radio talk show host and Guardian Angels founder, it is now run by Parry Aftab. Ms. Aftab is an Internet lawyer (having hosted AOL's Legal Discussions and created Court TV's Law Center's Legal Helpline), and author of *A Parent's Guide to the Internet* (SC Press 1997) and the newly released *The Parent's Guide to Protecting Your Children in Cyberspace* (McGraw-Hill, 2000), which was specially adapted for, and released in, the U.K. and Singapore in April and May, respectively. It is being adapted for Europe, South and Central America and Asia, as well, and translated into more than six languages, including Chinese, Japanese, Spanish and German.

Cyberangels operates through its volunteers, which now number more than 5,000. It is run virtually, online, in more than fourteen countries around the world. Its website contains safety and privacy information for adults, parents, teachers and children, including interactive quizzes, and fun safety cartoon characters, such as "Super Safe Kiddo." It also contains most of Ms. Aftab's first book, *A Parent's Guide to the Internet*, without charge.

Unlike other safety educational programs, however, Cyberangels also offers help to Internet users. Rather like a Cyber911, people who have encountered problems online, ranging from being hacked and infected with viruses, being cyberstalked and harassed, or encountering cyberpredators, to simply not understanding how to use their computers effectively online, or when they are seeking help with selecting and configuring parental control products, can all find immediate help from Cyberangels, via e-mail, instant messaging or in our help chats.

It maintains IRC help channels on most major IRC networks which are staffed during most hours by specially-trained IRC Ops. One of these channels, using a family-friendly IRC service, SuperChat, is available directly from the Cyberangels site, using a java-interface, allowing web-access to the IRC channel. This channel is staffed almost 24 hours a day, 7 days a week by Cyberangels IRC Ops, trained to handle online problems.

Cyberangels' volunteers apply online, and are trained online as well. Online classes are provided to anyone interested, without charge, ranging from "When is Your Child Old Enough to Chat" to "Protecting Your Privacy Online." They are also provided at special times to accommodate the special time zone needs of various international volunteers and site visitors. While it is a U.S. 501c3 non-profit, it operates online worldwide. It has, currently, four foreign language teams, principally to find and report child pornography online. The most active of its international and foreign language teams is Japan, which has been responsible for the first two arrests of alleged child pornographers in Japanese history. (The first took place a mere ten days following the implementation of their first child pornography law on November 1, 1999.)

Cyberangels is perhaps best known for its work with parents, teachers and children. Its Cybermoms and Cyberdads program trains parents in Internet safety and privacy, and provides offline programs for schools and community groups around the world. Its Teenangels program, run in conjunction with Wired Kids, trains teens in Internet safety, privacy and ethics and has created both a website written by teens, and a Teenangels Safety Ambassador program, where the specially-trained teens visit schools, and community groups to teach Internet safety and smart surfing. The first group of Teenangels have been invited to the Whitehouse to attend the ceremony when Cyberangels received its President's Service Award (selected by the Points of Light Foundation) and to teach various members of Congress about the Internet. A brief tape of their presentation to certain Congressional Representatives was shown at the launch of GetNetWise, in July, 1999. The Teenangels offline programs have been replicated in Japan, the U.K., Canada and Singapore, to date.

As well as teaching parents about safe surfing for their children, Cyberangels has also instituted programs for schools, building Internet safety and privacy into the school curriculum. Packets explaining risk management and the necessity for adoption of acceptable use policies and safe website practices have been distributed and will be distributed in schools around the world. Cyberangels also holds programs for school administrators on these issues, as well as on filtering and technological tools which are available, as well as their effectiveness. Working with large educational groups, its Smart Surfing programs have and are being adapted for the U.K., Singapore and Japan as well. Its Japanese program was first adopted by NEC Corporation, who made it their community service project for 1999, giving the employees of their twelve tech-related subsidiaries in Japan the day off, with pay, to deliver the program to parents and their children in Japanese schools. This program will be replicated here in the U.S. in October.

Cyberangels is a proud advisor to GetNetWise, and Ms. Aftab helped create the content at the GetNetWise site. Its Cyberangels Safe Site list is featured at GetNetWise, as well as Ms. Aftab's safe surfing contract. (This list is being regionalized worldwide to include sites that are Asian-centric and European-centric, as well as in other languages.) To dovetail with the extraordinary filtering tools resource of GetNetWise, Cyberangels has reviewed more than 120 filtering tools and services, and will be posting that information at the site. (GetNetWise doesn't review the products, but lists their features. This will give parents a sense of what other parents who used and tested the products thought.) In addition, Ms. Aftab's chart from her new book has tested the big four filtering tools against certain inappropriate site content to see how well they performed against hate, vs. satanic materials, vs. violence or bomb building. This appeared in the December Reader's Digest and will be posted along with the tool reviews, shortly.

Together with SOC-UM (Safeguarding Our Children – United Mothers), Cyberangels has compiled a copyrighted list of sites that advocate pedophilia or support pedophile groups. This list, known as KIDList (Kids In Danger List) contains approximately 45,000 websites. The list is available without charge to law-enforcement agencies, and for a licensing fee to filtering companies. Net Nanny is among the companies licensing the list.

Cyberangels also works very closely with law enforcement agencies around the world, including Hong Kong police, West Yorkshire police, Scotland Yard, the FBI, U.S. Customs Cybersmuggling Unit, the Royal Canadian Mounted Police and Japan's National Police and their Tokyo Metropolitan Police. It has more than 350 active law enforcement volunteers, and a special law enforcement division, run by a law enforcement officer volunteer. Its work has helped the FBI successfully prosecute many child molesters, helped law enforcement find children who have run off with Internet "friends" (recently helping return three in one week) and prosecute child pornographers and cyberstalkers. It runs training programs for law enforcement online and at police academies, and has been selected by the New Jersey Police Benevolent Association to train them in Internet safety for creating community and school programs, such as D.A.R.E.

Cyberangels is a main arm of UNESCO's online safety program, Innocence in Danger in North America. Ms. Aftab was named to chair the project by UNESCO. This resulted in the creation of Wired Kids (www.wiredkids.org) a consortium of commercial companies, non-profits and governmental groups who focus on equitable access, Internet safety and privacy and effective educational use of the Internet. Most, if not all of the experts testifying here today are members of Wired Kids. It was designed to allow groups to collaborate and share their work in the field of children online.

In response to the Columbine tragedy, Cyberangels set up its KIDReportline, a place where students can report threatening online behavior of their classmates. Too many children feel unable to report such behavior directly to their schools, but they are the ones most likely to know if a fellow classmate has a troublesome website and also to know if that particular classmate is likely to act on their online threats. The tips to the KIDReportline must come from children, and must relate to a fellow classmate's online website, which must display a credible threat of violence. Cyberangels does not keep any database of these tips. When a credible tip is received meeting all the conditions, Cyberangels alerts the appropriate authorities.

By making presentations to hundreds of parents and thousands of children and teens each month, Cyberangels stays on top of what they want and need. In addition, Ms. Aftab and it conducted (with Drs. Berson from the University of Central Florida) a survey of 10,800 teen girls, learning what they do and where they are at risk. It learned that 12% of the girls meet strangers offline, 48% share personal information with strangers online and 60% engage in some sort of graphic sexual discussions online. The Teenangels programs are designed to teach teens and preteens to use the Internet more intelligently.

In addition, Cyberangels works very closely with the FTC on COPPA matters, helping report sites which violate the law and educating schools, parents and children about Internet privacy. Together with corporate sponsors, Cyberangels has helped create educational bookcovers and posters on Internet safety, and online safety programs for schools around the world. The "Ask Parry" syndicated column is available without charge for any website which wants to provide online safety advice for their visitors. Cyberangels will screen questions from those sites and select a few each week for Parry to answer in her column. The column can then reside that those sites.

A recent article from Reader's Digest is being supplied in reprints for your review on work Cyberangels does for adults and teens who are victims of cyberstalking, as well.

Any questions can be directed to Ms. Aftab, at parry@aftab.com. The Cyberangels site is found at www.cyberangels.org.

Reader's Digest
UNITED STATES

7.99% APR It's like car-shopping with CASH! CarsDirect

Are you getting the most out of your PC? free CD Rom! Reader's Digest BOOKS

November 8, 2000
Books Music Videos Magazines Online Store Customer Service

International Sites

RD Online
Home
Article Archives
Letters
Select Editions
Humor
Word Power
RD Kids
Hangman
Discussions

Help Center
Customer Service
Contact Us
Corporate Info
Privacy Policy
Reprints
Advertising Info
Affiliate Program
Terms of Use
RD Web Sites

Our Other Magazines

SPECIAL REPORT

Protect Yourself Online

How easy is it for a stranger to get personal information about you online? Can you use the Internet anonymously? Writer Hal Karp spoke with Parry Aftab, executive director of CyberAngels, about these questions and more.

By Hal Karp

Special Report - "Angels Online"
Join The Debate
Related Links

How vulnerable are people online?

More vulnerable than most realize. When people go online they are too trusting and naive when it comes to personal information. Most share information that they would never give someone they met casually off-line. Would you tell the person standing next to you in the grocery store check-out line your address and phone number? Of course not, but it's no different than doing so in a chat room, often unknowingly.

How would you do so unknowingly?

Many chat programs and Internet service providers ask you to fill out a profile about yourself. What most people don't know is that this information is frequently available to anyone who wants to see it online. So if you fill out your profile with detailed information about your life, you're vulnerable. Also, say you're chatting with someone and tell them you last name and what city you live in. All they have to do is search one of many databases available on the Net to locate more information about you. They could easily locate you with only a last name. The amount of personal information available on the Web regarding people is astonishing.

How else can you protect your personal information?

Whenever you fill out any form online, check to see what the site's privacy policy is. Who will see your information? Will it be sold? If it's open to others' eyes, don't fill in the blanks. And if you've created your own website, don't feature any personally identifiable information. This would include pictures with identifiable features such sweatshirts with school names and recognizable landmarks. And certainly don't post your personal address on your site. Just ask yourself, "Is there anything on my site that could help someone find me?" If there is, get rid of it.

Are there other steps to take that can make it difficult for someone to find you?

Absolutely. Most people don't know that there are abundant directories and databases online that list their addresses, email addresses and phone numbers. Several directories now boast reverse look-ups. This is where I can type in your email address and find out who you are, or do the same with your phone number and address. I can even find out who your neighbors are. In some states, I can pull-up your driver's license onscreen. So the trick is to get your information removed from as many of these databases as possible. Start by searching for yourself, everywhere you can. If you can find you, so can they.

Reader's Digest

Click here for a chance to win $125,000.00!

pledge for a brighter future Click here

Apply Now! 60 Second Response*

Special Offers
Free Book Offer
Free Travel Info
2001 Day Planner - $5

Additional Sites
Site Seeing
Just the perfect gifts! gifts.com
The Good Catalog
RD Insurance

Announcements
Fiscal 2001 1Q Earnings
RD Annual Report 2000

What other common mistakes do people make online?

They don't learn the rules before venturing into cyberspace. They don't look before they leap into a chat room or onto a discussion board. In such scenarios, you can easily break the rules and upset others. And you never know who's angry until it's too late. Off-line we all know the rules of proper social etiquette. However, online most don't know that there is a similar set of rules we call Netiquette. These rules are necessary for staying out of trouble. A lot of cyberstalking cases occur when people inadvertently bend or break these rules. To enter an established and unknown chat room and interrupt ongoing conversation to draw attention to yourself should be seen as no different than wandering into a bar or a party where you weren't invited and don't know anyone. Would you draw attention to yourself there?

Can you further explain Netiquette?

Netiquette is simple. We're talking about correct behavior, which should be the same online as it is off-line. Basically show respect for others and avoid anything that hints of trouble. If you break the accepted rules of Netiquette, often people deputize themselves to correct you by teaching you a lesson. Often this is done the hard way. We tell people, "Just don't park your common sense at the computer when you get online."

Is it possible to email someone or surf anonymously?

Yes. You can use a free service like Anonymizer which cloaks you completely. Any Web site you've visited will not be able to trace your Internet service provider. To play it safe with email, use a free web-based email account such as Hotmail when writing to strangers. There are many such services. This way no one can track where you live by tracing your Internet service provider who might be local only to your city.

Any safety tips for chatting online?

The safest place to chat is in a chat room with people you know off-line. This may sound odd, but kids do this a lot. They get home and get online with the people they just left at school. Otherwise use a genderless, non-provocative screen name and remember that the moment you get into a chat room with people you don't know, be careful. Keep in mind, these are strangers you're talking to. They may sound friendly, but online anyone can be anything they want. You shouldn't share confidences with them anymore than you would with a stranger sitting next to you on the bus. If you do, you're putting yourself at risk.

Continue on to page two of the interview

E-mail this page to a friend

Copyright© 2000 The Reader's Digest Association.

Home | Article Archives | Letters To The Editors | Humor | Wordpower
Hangman | Discussions | Select Editions | RDKids | Customer Service
Contact Us | Corporate Info | Privacy Policy | Reprints | Advertising Info
Become an Affiliate | Legal Terms of Use | RD Websites
Reader's Digest Magazine

Copyright© 2000 The Reader's Digest Association.

ERNIE ALLEN
BIOGRAPHICAL INFORMATION

Ernie Allen is President & Chief Executive Officer of the National Center for Missing & Exploited Children. He was co-founder of the private, nonprofit Center, which has helped recover 50,000 children, while increasing its recovery rate from 62% in 1990 to 93% today.

Allen has brought technology and innovation to the Center, including computerized age progressions of long-term missing children; an award-winning Internet website that handles 3 million "hits" per day; a CyberTipline called "the 911 for the Internet;" and a new International Centre to expand services worldwide.

Under his leadership, the Center has grown from a $3 million organization in 1989 to a $38 million organization today with offices in six states and the United Kingdom. The Center is one of only ten national charities graded "A+" by the American Institute of Philanthropy.

Ernie Allen is an active spokesman for the cause, having made numerous appearances on Oprah, The Today Show, Good Morning America, Larry King Live, and many others. He was named "1998 Communicator of the Year" by the National Association of Government Communicators.

Ernie Allen came to the Center following public service in his native Kentucky, where he was Chief Administrative Officer of Jefferson County, Director of Public Health & Safety for the City of Louisville, and Director of the Louisville-Jefferson County Crime Commission.

He is an attorney and member of the Kentucky Bar; and a teacher, having held faculty positions at the University of Louisville, University of Kentucky, and Indiana University.

He has been honored by his alma mater, the University of Louisville, as Distinguished Alumnus of the Louis D. Brandeis School of Law, and Outstanding Alumnus of the College of Arts & Sciences.

Testimony Outline of
Ernie Allen, President
National Center for Missing & Exploited Children

COPA Commission Hearing
Thursday, June 8, 2000
"Resources for Families that are One Click Away" Panel

I. *Online Victimization: A Report on the Nation's Youth*
  A. Congress's Request for Data
  B. Major Findings

II. CyberTipline
  A. Background
    –funding
    –how it works
    –mandatory ISP reporting
  B. Status (attachment 1)
  C. Effectiveness (attachment 2)

III. Recommendations

Attachment 1

CyberTipline Status

CyberTipline Weekly Activity Report #116 (May 29 - June 4, 2000)

Type of Incident*	Weekly	Project to Date
Child Pornography	241	16,809
Child Prostitution	7	436
Child Sex Tourism	1	275
Child Sexual Molestation (not in the family)	16	1,139
Online Enticement of Children for Sexual Acts	23	2,491
Total # of Reports	288	21,150

*As selected by reporting person/caller when completing this form.
**Blank Reports: 336 (project to date)

Online Service Provider Referrals

	Weekly	Project to Date
CT Reports sent to AOL	2	566
CT Reports sent to Compuserve	--	1

ISP Referrals to CyberTipline

	Weekly	Project to Date
Bell Atlantic	--	2
UUNet	--	5

European Hotline Referrals to CyberTipline

	Weekly	Project to Date
Internet Watch Foundation (UK)	--	29
Belgium Judicial Police	--	24
Meldpunt (Netherlands)	6	306
ISPA (Austria)	--	67
ISPAI (Ireland)	--	10
AFA (France)	1	10

CyberTipline Effectiveness

Following are recent "success stories" resulting from CyberTipline reports. The examples illustrate how NCMEC's Exploited Child Unit (ECU) analysts respond to child sexual exploitation reports and how they work with federal, state, and local law enforcement to provide the most usable information for investigation purposes.

> **Florida, May 2000:** An anonymous report to the CyberTipline provided a URL to a child pornography site. ECU analysts accessed the site and confirmed that several images of child pornography were located in various subdirectories. The site also advertised additional images of child pornography and linked to additional child pornography sites that were located on different IP addresses. An Internet search conducted on the domain name for the reported web site led ECU analysts to an individual in Tallahassee, Florida, who was using a post office box address. ECU analysts forwarded the information to the Sex Crime Unit at the Tallahassee Police Department. On May 5 the suspect was charged with 22 felony counts of promoting sexual performance by a child.
>
> **California, March 2000:** A child's mother reported online that she just learned that a family friend molested her 14-year-old daughter when the child was 11-years old. The 54-year-old suspect fondled the child during a sleep over at his house. The child was a friend of the suspect's son. ECU staff contacted the reporting person (RP) to gather additional information on the case and then forwarded the report, along with AutoTrack search results, to local law enforcement in California. The assigned detective recently contacted NCMEC to report that the suspect, after admitting to the molestation, was arrested on March 4 for two felony counts of child sexual molestation.
>
> **New York, March 2000:** ECU staff received a report from a mother whose 13-year-old daughter and her daughter's 13-year-old friend had traveled from the Bronx, New York, to Staten Island, New York, to meet two adults they had been corresponding with online. Upon their arrival in Staten Island, the adults engaged in sexual activities with the girls. The reporting person contacted NYPD, and upon the advice of law enforcement, took her daughter to be medically examined. The exam confirmed that molestation had occurred. ECU staff conducted AutoTrack searches on the suspect's pager and phone numbers as well as conducting Internet searches on his e-mail address. ECU staff contacted the NYPD and offered assistance regarding the Internet-related aspect of this case. Local law enforcement then informed NCMEC that both suspects had been arrested.
>
> **North Carolina, March 2000:** ECU analysts received a report about a 44-year-old man who was contacting the reporting person (RP) and asking her to run away with him because he thought the RP was a 15-year-old female. Because no suspect information was received, ECU staff contacted the RP and received additional information about the incident and the suspect's e-mail address. ECU analysts reviewed an online profile for the suspect and from the identifying information they were able to query a public records database for additional location information for the suspect. ECU staff confirmed the suspect was residing in the state indicated on his profile and the suspect was using a post office box address. ECU analysts contacted the U.S. Postal Inspection Service about this

report. The Postal Inspector began an online investigation acting as the fictitious 15-year- old female. The suspect was arrested on March 23 after traveling from North Carolina to Fredricksburg, Virginia, to have sex with the fictitious child. The suspect was charged federally for traveling in interstate commerce for the purpose of having sex with a person under the age of 18.

Ohio, February 2000: A citizen reported to the CyberTipline that he had been sent child pornography. The sender of the images claimed to be the adult in the pictures and stated that his 40-year-old friend was also molesting one of the boys in the images. The citizen was advised to contact his local FBI field office to determine the right course of action for transferring the evidence to law enforcement. ECU analysts uncovered several e-mail accounts, newsgroup postings, a web site, an ICQ account, and an Akron address for the suspect. The Akron Police Department and the Ohio Attorney General's Office were notified. Police arrested the suspect at work and executed a search warrant at his home. The suspect has been charged with the rape of two boys, corruption of a minor (for a third boy) and pandering sexually oriented matter on the Internet.

Florida, February 2000: A Florida mother reported that her son had recently disclosed that his baseball coach was touching him inappropriately when they were away on camping trips. ECU staff contacted the caller and gathered additional information regarding the suspect's contact with her son and the children on the team. ECU analysts became aware of an additional child victim and spoke with the second mother regarding her son's recent disclosure. ECU staff confirmed the suspect's Florida address using public records databases, and forwarded the CyberTipline report to local law enforcement and the Florida Department of Law Enforcement. Days later, ECU spoke with the local investigating officer and was told that the case was suspended. Days later, the RP contacted the ECU analysts and stated there was another child who had recently disclosed additional information about the suspect. Again, ECU advised the RP to get the child's mother to call so that the additional information could be added to the original CyberTipline report. ECU spoke with the third mother and added supplemental information to the report regarding her son's recent behavior changes and a disclosure he made. This report was sent out to a new investigator with the local law enforcement agency and to FDLE. On February 26 the suspect was arrested and is being charged with three counts of lewd and lascivious behavior.

Alabama, January 2000: A person reported to the CyberTipline the alleged molestation of her 9-year-old niece by the niece's mother's boyfriend. The mother denied the abuse. ECU staff ran searches on the suspect and found information on his residency for the past four years. ECU staff spoke with the reporting person (RP) and gained additional information about the incidents, the child's disclosure, the medical examination of the child, and law enforcement's current involvement in the case. ECU analysts provided the RP with several different victim resources and encouraged the RP to have the child's biological father and stepmother make a report directly to law enforcement. ECU contacted the Sheriff's Office and explained the case and the urgency of getting this information out prior to the weekend, since the child was still in contact with the suspect. The report was then faxed to the Sheriff who had jurisdiction in the case. An officer with the local police department then contacted ECU and informed us their department currently had two arrest warrants for the suspect on child abuse charges. He also stated that the Sheriff's Office would be filing a separate search warrant for first-degree rape charges. However, at this point they were uncertain of the suspect's location. ECU provided law enforcement with the suspect's residential information from the national comprehensive search on AutoTrack. The following day, the officer at the police department called to inform the ECU that the suspect was incarcerated in the Fayette County (AL) jail.

Wisconsin, November 1999: Based on a CyberTipline report from a European child pornography hotline, ECU analysts confirmed a site with images of children engaged in sexual activities with adults and other children. An ECU analyst's search results indicated that the creator of the web site resided in Wisconsin, and public records searches provided an address for the creator. ECU staff contacted the Wisconsin Division of Criminal Investigation's Internet Crimes Against Children Task Force to alert them to this information. Upon receipt of the CyberTipline lead, the task force executed a search warrant at the 17-year-old suspect's home. Based on evidence seized, the suspect is facing felony counts for the possession of child pornography.

Michigan, September 1999: An anonymous CyberTipline report led ECU analysts to find graphic child pornography of female children under the age of eight online. Using various Internet search tools, ECU analysts identified the suspect, reviewed his profile, and ascertained his age, location, and other critical identifying information. This data was utilized to perform further queries that provided the suspect's first name, last name, and his exact date of birth. ECU transmitted the information to the Michigan State Police, who executed a search warrant at the suspect's residence. Evidence collected included over 1,250 photos depicting young girls in sexually explicit positions and 14 video files that show girls as young as 5-years-old being sexually abused by adult males. The suspect was using approximately 10 e-mail addresses to communicate online.

Dr. Lawrence J. "Larry" Magid

A syndicated columnist since 1983, Magid's twice-weekly columns originate in The *Los Angeles Times* and appear in newspapers and on web sites throughout the world. He also serves as CBS News Computer Consultant. His technology reports can be heard several times a week on CBS Network and CBS affiliates throughout the United States.

Larry also writes columns for *Microtimes* and Upside.Com. He has also written for *Fortune, ForbesASAP, Family Circle, PC World, PC Magazine, Information Week, Modern Maturity, Computer Currents*, *ComputerWorld* and numerous other publications.

In addition to his work for CBS network, Larry's technology commentaries can be heard daily on both KNX (CBS Los Angeles) and KCBS in San Francisco. He is host of the Palo Alto Cafe which can be heard on Redband Broadcasting's website and on public radio stations. He is also co-host of The World Wide Web Radio Show a nationally syndicated radio show distributed by Talk Radio Network. He is also heard occasionally on National Public Radio. He can also be seen on The Internet Café, which is aired on more than a 160 U.S. public TV stations, as well as on NBC Europe and he is a regular pundit on ZDTV's Silicon Spin program. Larry has made repeat appearances on The Larry King Show, CBS This Morning, NPR's Talk of the Nation Science Friday, All Things Considered and many other programs.

He is the author of several books including *The Little PC Book* (now in its 3rd edition), a critically acclaimed best seller, *The Little Quicken Book, Cruising Online: Larry Magid's Guide to the New Digital Highways* (Random House, 1994), *The Fully Powered PC* (Simon and Schuster, 1984) and *"Electronic Link: Using the IBM PC to Communicate*" (John Wiley and Sons, 1983). He is also the host of three popular web sites: LarrysWorld.com, SafeKids.com and SafeTeens.com.

Larry served as editor during the early days at *PC* magazine and was co-founder of Know How, one of the nation's first computer training companies. He has served as a commentator for CNN's Computer Connection and as Managing Editor of The Computer Show, a syndicated television program.

Larry is the recipient of the National Center for Missing and Exploited Children's "Ten Year Anniversary Award" for his work in developing a system for finding missing children via online services. TIME magazine (November 1, 1993) called Magid and his colleagues "high tech heroes" for that work. Magid serves on the board of directors of Telis, a non-profit educational foundation dedicated to improving network access for all, including low-income and disadvantaged families. Magid's web sites, SafeKids.Com and SafeTeens.Com were selected as Laureates in the prestigious 1999 Computerworld/Smithonian award.

Magid is the author of Child Safety on the Information Highway, a free booklet that has helped millions of families understand how to safely navigate cyberspace. His newest booklet, *Teen Safety on the Information Highway* was published in March by the National Center for Missing and Exploited Children. He is also author of the safety guide on the GetNetWise.Org child safety web site. In an earlier life he was editor/publisher of *EdCentric*, a leading journal of educational reform and served as director of the National Student Association's Center for Educational Reform.

Larry doesn't play a doctor on TV but he does have a doctorate of education from the University of Massachusetts and has taught at the University of Massachusetts and the Boston University School of Communications.

SafeKids.Com

SafeKids.Com / SafeTeens.Com testimony before COPA Commission.
June 8, 2000

Presented by Dr. Lawrence J. Magid, founder and editor-in-chief
Contact: larry@safekids.com /650 813-9478. Cell phone: 888 713-9478

Introduction

SafeKids.Com and SafeTeens.Com were founded in September 1998 to serve a very simple function: Help kids, teens, parents, educators and law enforcement develop strategies for keeping kids safe on the Internet. Although the sites are not affiliated with the National Center for Missing and Exploited Children or any other organization, some of the material contained on the sites is based on the Center's brochures, Child *Safety on the Information Highway* and *Teen Safety on the Information Highway* that were written for the Center by SafeKids.Com founder, Lawrence J. Magid. Likewise, the sites are not affiliated with GetNetWise.org, but Dr. Magid helped develop GetNetWise's safety material and both SafeKids.Com and SafeTeens.Com support and link to the GetNetWise site.

The goal of SafeKids.Com and SafeTeens.Com is not to promote any specific technologies or techniques for assuring safety but to get families to think about a variety of issues. The project maintains a separate site for teens because, though they may be minors, teens are not children. They have different risks and different needs and different strategies are needed to help them protect their own safety in cyberspace.

Speaking of differences, both sites operate on the assumption that different families have different values and need different strategies to assure their safety. Yet, there is one overriding theme that extends throughout much of the material on both sites. Parents and other caregivers are urged to help children and teens develop critical thinking skills so that they, ultimately, can protect themselves not only in cyberspace but also in off-line world. Knowing how to act defensively, avoiding dangerous places and thinking critically can serve your children well on dates, in the marketplace, in the car and in the voting booth as well as on the Internet. Rather than approach Internet safety as purely a problem, think of it as an opportunity.

SafeKids.Com has extensive information about Internet filtering software and filtered Internet Service Providers but the site does not necessarily recommend the use of such technology for all families. In some cases, filtering technology is clearly the right choice but in other situations, it may be inappropriate. Every parent must make the decision for each of his or her children. What might be a very smart move in one home could be inappropriate in another. There are even differences within families. What is appropriate for one child might not be appropriate for a sibling, even if the two children are approximately the same age.

Filters for the Brain

Regardless of whether a parent chooses to use technology to help control what a child or teen says or sees on the Internet, ultimately, the best safety filter runs not on a computer but in the young person's head. Kids and teens need to learn how to protect themselves. While close parental supervision is a must for young children and filters are appropriate in some circumstances, the child's and teen's attitude is ultimately more important.

Using an automobile safety analogy that we're all familiar with, active restraints, like seatbelts, save lives but they are useless if not deployed. Even passive restraints, like airbags, are no substitute for defensive driving And, as appropriate as it is to hold a young child's hand when he or she crosses the street, parents must ultimately prepare their kids for the time when they must fend for themselves. The same is true on the Internet. Regardless of whether a parent uses a filter at home when a child is young, the child will -- probably sooner rather than later -- have unfiltered access to the net. It could be at school or a library or a friend's house or later in life. The child's ability to make good decisions is what will provide the best protection.

Distinguishing Safety from Social and Moral Issue

One of the most pressing needs in the arena of Internet safety is to distinguish the various issues. SafeKids.Com and SafeTeens.Com focus primarily on the issue of safety but recognize that some parents have other concerns including wanting their children's access to the net to reinforce family social and moral values. As important as these values are to many families, they should not be confused with safety. That isn't to say that such issues as access to pornography should be ignored by those of us who are concerned with children and the Internet. However, it is important to remember that "protecting" a child from deliberately accessing information that his or her caregiver considers to be age inappropriate is not the same as protecting a child from physical danger, harassment or criminal acts.

It is also important to draw a distinction between the protection of children and moral and social issues that affect adults. We respect the point of view of organizations that strive to help adults avoid or recover from obsessive use of sexually explicit material but feel that such campaigns should be kept separate and distinct from programs to protect children. Likewise, it is important to distinguish between child pornography and children's access to pornography that is otherwise legal.

Finally, it is important to remember that some of those who prey on children are in fact, also children. Data from the National Center for Missing and Exploited Children's "Online Victimization Study" show that 48% of the perpetuators of sexual solicitations to people between 10 and 17 are themselves under 18 and that only 4% of such solicitations are known to come from people over the age of 25. This data suggests that, in addition to educating young people to avoid becoming victims, we must also educate them to avoid victimizing others. While it may not impact physical safety, courses on "netiquette" are indeed called for. The data further shows that the Internet is a microcosm of society as a whole, suggesting that we -- as a nation -- have a larger agenda when it comes to teaching young people to be more respectful of others.

Measured Responses

One of the major goals of SafeKids.Com and, especially, SafeTeens.Com is to help parents develop appropriate responses to problems associated with the Internet. Young people should be encouraged to come to their parents if they encounter material that makes them feel uncomfortable or are solicited in inappropriate ways. Over reacting or taking away Internet privileges could prove to be counterproductive, sending the message that it's not OK to confide in your parents. To that end, we are providing resources and educational materials to help parents lend an understanding ear to kids rather than "blame the victim" when a young person brings a problem to their attention.

It is also important to realize that children have rights. It is beyond the competence of SafeKids.Com and SafeTeens.Com to adjudicate between a teenager's right to free speech and association and a parent's responsibility to govern their children's online and offline behavior. Nevertheless, as murky as these lines may be, it is important to be cognizant of the rights and responsibility of young people, especially as they approach adulthood.

Let a Thousand Safety Sites Bloom

SafeKids.Com and SafeTeens.Com do not exist in a vacuum. The sites are part of a larger community of child safety resources, each of which brings different information, resources and perspective. The two sites have numerous links to other sites with online safety information as part of a concerted effort to encourage parents to explore a variety of resources and perspectives.

Getting the Word Out

Like any other successful website, SafeKids.Com and, to a lesser extent, SafeTeens.Com take advantage of a number of promotional opportunities. Although neither site spends any funds on marketing or advertising, both enjoy widespread recognition via the media and through links from other sites.

SafeKids.Com has received extensive and ongoing media coverage in such places as CBS Television and radio, ABC News, Women's Day, Family Circle, Associated Press, CNN, FamilyPC, the Los Angeles Times, the San Jose Mercury News, USA Today, the Miami Herald and numerous other news and information outlets in the U.S. and in other countries. Also, SafeKids.Com was singled out by the producers of CBS TV's "Touched by an Angel" for an unsolicited free public service announcement that appeared on screen after an episode about dangers on the Net. SafeKids.Com has also been heavily promoted by Yahoo, Lycos and other search engines. An analysis using WebsiteGarage.com shows that SafeKids.Com has links from nearly 1,100 other sites, giving it the highest "link popularity" of any website dedicated to keeping kids safe on the Internet.

Keeping Up To Date

SafeKids.Com is updated about once a week. Appropriate safety related articles from Lawrence Magid's Los Angeles Times and San Jose Mercury news columns are regularly along with other material. What's more, SafeKids.Com, in cooperation with NetFamilyNews, sends out a weekly e-mail newsletter that covers not only Internet safety but also a wide variety of other issues of interest to families and educators.

Roger Cochetti
Senior Vice President and Chief Policy Officer
Network Solutions, Inc.

Roger Cochetti is Senior Vice President and Chief Policy Officer of Network Solutions, Inc. In that position, he is NSI's spokesman to, and liaison with, U.S. and non-U.S. governments, the Internet Corporation for Assigned Names and Numbers (ICANN) and to the Internet and electronic policy communities. Roger joined NSI in February of 2000. He is a globally-recognized leader in the field of policy and regulation of electronic commerce.

Before joining NSI, Roger Cochetti was Program Director - Internet Policy and Business Planning for IBM Corporation, where he led IBM's global activities in the e-commerce policy field, including such areas as the regulation of content, privacy, taxation, e-mail, and trade on the Internet. Earlier, he had managed the business development activities of IBM's Personal Communications Services unit. From 1981 through 1993, Roger was with Communications Satellite Corporation (COMSAT), where he served as Vice-President-Business Development & Planning for COMSAT Mobile Communications. In that position, he directed the business' strategic planning, pricing, and M&A activities, including major joint ventures in Turkey, Japan, and Malaysia, as well as in several global, satellite consortia. Earlier, he had directed COMSAT's Corporate investor and public relations activities. Prior to joining COMSAT, Roger served as an official in the United States Department of State, where he was Assistant Director-Legislative & Public Affairs of the U.S. Development Cooperation Agency (IDCA), the principal Federal agency responsible for US foreign aid programs.

Roger serves on the boards of a variety of Internet-related publications, organizations, and companies, including the Editorial Advisory Board of e-Business World, TRUSTe, the Internet Law and Policy Forum, and the Internet Education Foundation (the private sector affiliate of the Congressional Internet Caucus) and many others. He is a frequent commentator on e-commerce policy topics.

Roger Cochetti is a graduate of Georgetown University and is the author of a book and numerous articles on Internet and telecommunications topics. He lives with his wife, Mary, and sons, Andrew and Emmett, in Chevy Chase, Maryland.

SUMMARY OF REMARKS ON INTERNET TOP-LEVEL DOMAINS

TO THE COPA COMMISSION

ROGER J. COCHETTI, SENIOR VICE-PRESIDENT

NETWORK SOLUTIONS, INC.

- Top level domains (".com", ".gov" or ".uk") are important guideposts in the Internet and they help users navigate a medium that could otherwise be too complex
- In 1998, the Internet Corporation for Assigned Names and Numbers (ICANN) was created to, in part, address Internet administrative matters
- NSI has been supportive of the creation of new global TLD's and has encouraged ICANN to do so rapidly, but with due care and caution
- While all TLD's are technically equal signposts, they have evolved along fairly different lines: country code TLD's; global TLD's; and special TLD's
- This evolution has caused considerable controversy as precise definitions are developed and refined (e.g. the difference between "open" and "closed" TLD's)
- Nowhere has the controversy been greater than in proposals to create either new global TLD's, particularly if they are "open"
- Open, globally-accessible TLD's raise important trademark infringement issues, which have been the subject of study by WIPO and other since 1997
- Chartered, or closed TLD's trend to raise fewer trademark questions than they do enforcement questions
- Ultimately, the Internet is a global medium (over half of its users are non-American) and thus it must be administered globally or it will degenerate
- Finding globally-acceptable mechanisms to administer chartered TLD's has been a daunting task, partly because of national industrial policies
- Another major obstacle to the establishment of chartered TLD's has been cultural differences: people in different societies see things/terms differently
- For example, in order to illustrate how we thought a new chartered TLD might be organized quickly, we suggested the concept of a ".banc" TLD
- It did not take long to understand that, even with the use of a fairly loose term like "banc" (vs. the word "bank") there were many different perspectives globally
- It is in this context that we have examined the idea of creating a ".sex" or similar adult-oriented domain on a global scale

- We have no objection to the creation of an adult TLD, however it is clear that doing so internationally raises more issues than if it were done only for the U.S.
- This could be done under the ".US" TLD, which has not been very much exploited, and is the subject of a current Commerce Department review
- If an adult TLD were to be created on a global scale, it could be either open to anyone who wished to register in it or open only to certain registrants (i.e.closed)
- If it were open, then it would raise fewer issues of finding a common definition, although it might not be easy to find a commonly agreed upon word
- But any open TLD will raise important trademark infringement issues, whether it is for adults or not
- If it were closed (sometimes called "chartered") in the sense that only certain types of registrations would be permitted, then major administrative issues arise
- Who would define who may register and who may not? Who resolves disputes over compliance? Who should be the gatekeeper for such a TLD?
- Moreover, adult material is subject to extensive regulation in most countries and - depending on the definition used- is illegal in others
- Accordingly, it is likely that by simply registering in an adult TLD, a registrant would subject themselves to investigation (perhaps prosecution) in some countries
- At a minimum, there would be some temptation for some governments to require that adult material be posted only in an adult TLD
- Conversely, if a registrant whose site posted adult material failed to locate that site in an adult TLD, could they then be prosecuted for failing to give adequate notice of the adult nature of their site?
- These are complex questions that would take some time to sort out even if the TLD were for American only. Any global TLD would be more complex.
- In sum, we at NSI are supportive of the creation of new Internet TLD's and have urged rapid expansion with due care and caution
- We have no objection to the creation of an adult-oriented TLD, but recognize and ask others to recognize, that it raises complex international questions that will take some time to understand and address. These would be fewer if the TLD were only for Americans.
- We're happy to support the Commission in its further work in this area

Roger J. Cochetti
Senior Vice President-Policy

Network Solutions, Inc.
rogerc@netsol.com

JONATHAN WEINBERG
jon@threecats.net
http://www.threecats.net

Wayne State University Law School
Detroit, MI 48202
(313) 577-3942

EMPLOYMENT

Wayne State University Law School 468 West Ferry Mall Detroit, MI 48202	Professor, 1999-present Associate Professor, 1993-99 Assistant Professor, 1988-93
Cardozo School of Law Yeshiva University 55 Fifth Avenue New York, NY 10003	Visiting Scholar, Howard M. Squadron Program in Law, Media and Society, spring 2000
Federal Communications Commission Office of Plans and Policy Washington, DC 20554	Legal Scholar in Residence, 1997-98
U.S. Department of Justice Civil Division (Appellate Staff) Washington, D.C. 20530	Professor in Residence, 1993-94
Shea & Gardner 1800 Massachusetts Avenue NW Washington, DC 20036	Associate, 1987-88 and 1984-85
University of Tokyo Institute of Journalism and Communication Studies Hongo, Bunkyo-ku, Tokyo 113, Japan	Visiting Scholar, 1986-87
The Hon. Thurgood Marshall Supreme Court of the United States Washington, DC 20543	Law Clerk, 1985-86
The Hon. Ruth Bader Ginsburg United States Court of Appeals District of Columbia Circuit Washington, DC 20001	Law Clerk, 1983-84

EDUCATION

Columbia Law School J.D. 1983
New York, NY 10027

* Writing and Research Editor, Columbia Law Review (Head of Notes and Comments Department)
* 1982-1983, 1980-1981 James Kent Scholar; 1981-1982 Harlan Fiske Stone Scholar
* Class of 1912 Prize (Contracts)
* Young B. Smith Prize (Torts)
* Charles Bathgate Beck Prize (Property)
* Robert Noxon Toppan Prize (Constitutional Law)
* Consolidated Edison Essay Award (First Amendment)

Harvard College A.B. 1980
Cambridge, MA 02138

* Graduated cum laude, concentrating in Government.

PUBLICATIONS

*Communications Law: Cases and Materials (in progress; should be finished in Summer 2000)

*ICANN and the Problem of Legitimacy (in progress; for publication in Duke L. Rev.)

*Internet Governance (in Japanese; Itsuko Yamaguchi trans.), in Cyberspace Law (Makoto Ibusuki ed. 2000).

A substantially revised version of this chapter is forthcoming in an English-language edition of the book; an Italian-language edition is also Scheduled for publication.

*Hardware-Based ID, Rights Management, and Trusted Systems, 52 Stan. L. Rev. — (forthcoming 2000).

A shortened and revised version of this article will be published in Victor Bouganim et al., The Commodification of Information: Political, Social and Cultural Ramifications (forthcoming 2001).

*Broadcasting and Related Media, in Encyclopedia of the American Constitution (Supplement II) (Leonard W. Levy, et al., eds.) (forthcoming 2000)

*The Internet and "Telecommunications Services," Universal Service

Mechanisms, Access Charges and Other Flotsam of the Regulatory System, 16 Yale J. on Reg. 211 (1999).

This article will also be published in Internet Telephony (Lee McKnight ed., forthcoming 2000); an earlier version of the article appears in Competition, Regulation and Convergence: Current Trends in Telecommunications Policy Research 297 (Sharon Gillett and Ingo Volgelsang, eds. 1999).

*US Media Law Update, 4 Media & Arts L. Rev. [Australia] 199 (1999)

*The New Broadcast Regulation (in progress, if I ever get back to it)

*Technology, Free Expression and the Law, Update on Law-Related Education, Fall 1998, at 6

*New Media and Old Debates (review of Rationales & Rationalizations: Regulating the Electronic Media (Robert Corn-Revere ed. 1997)), Jurist Books-on-Law (July 1998), available at <http://jurist.law.pitt.edu/lawbooks/revjul98.htm#Weinberg>

*Rating the Net, 19 Hastings Comm/Ent L.J. 455 (1997).

This article has also been published in The V-Chip Debate: Labeling and Rating Content from Television to the Internet 221 (Monroe E. Price ed. 1998); an earlier version appears in Interconnection and the Internet (Gregory L. Rosston & David Waterman eds. 1997).

* Cable TV, Indecency and the Court, 21 Colum.-VLA J.L. & Arts 95 (1997)

* The Telecommunications Act of 1996 and U.S. Media Ownership, in 1996 Yearbook of Media and Entertainment Law 99 (Eric M. Barendt et al. eds.) (with Monroe Price)

* United States, in Media Ownership and Control in the Age of Convergence 265 (Int'l Inst. of Communications 1996) (with Monroe Price)

* Vagueness and Indecency, 3 Vill. Sports & Ent. L. J. 221 (1996)

* Broadcasting and Speech, 81 Calif. L. Rev. 1101 (1993)

This article also appears in First Amendment Law Handbook, 1994-95 Edition 177 (James L. Swanson ed. 1994), and (without footnotes) as Hoso to Genron, in Hososeidoron no Paradaimu [Paradigms of the Broadcasting System] 79 (Junichi Hamada ed. & Itsuko Yamaguchi trans., University of Tokyo 1994).

* Broadcasting and the Administrative Process in Japan and the United States, 39 Buffalo L. Rev.615 (1991)

A substantial portion of this article appears in Michael H. Botein, Regulation of the Electronic Mass Media: Law and Policy for Radio, Television, Cable and the New Video Technologies 585-97 (3d ed. 1998).

*Thurgood Marshall and the Administrative State, 38 Wayne L. Rev. 115 (1991)

*Limiting Access to the Broadcast Marketplace, 44 Bull. of [Univ. of Tokyo] Inst. of Journalism & Comm. Stud. 2 (1991)

*Questioning Broadcast Regulation (review essay), 86 Mich. L. Rev. 1269 (1988)

*Amerika Gasshukoku ni Okeru Yusen Terebijon to Chosakuken [Cable Television and Copyright in the United States], 15 Chosakuken Kenkyu 23 (1988)

*Note, Constitutional Protection of Commercial Speech, 82 Colum. L. Rev. 720 (1982)

GOVERNMENT TESTIMONY

*Domain Name System Privatization: Is ICANN Out of Control?: Hearings Before the Subcomm. on Oversight and Investigations of the House Comm. on Commerce, 106th Cong., 1st Sess. (July 22, 1999)

*A New FCC for the 21st Century, en banc hearing before the Federal Communications Commission, June 11, 1999

PRESENTATIONS AND WORKSHOPS

*Freedom and Privacy by Design (invited workshop participant), Conference on Computers, Freedom & Privacy, Toronto, Canada, April 4, 2000

*Free Governance, Conference on A Free Information Ecology in the Digital Environment, New York University Law School, April 2, 2000

*Global ID, Trusted Systems, and Communications Markets, John Evans Lecture Series, University of Michigan, March 23, 2000

*Legal and Social Implications of Trusted Systems and Hardware Identifiers, Inaugural Annual Symposium on Internet, Law and Society, Cardozo Law School, March 22, 2000

*ICANN and the Problem of Legitimacy, 30th Administrative Law Conference, Duke Law School, March 3, 2000

*Hardware-Based ID, Rights Management, and Trusted Systems, Conference on Cyberspace and Privacy: A New Legal Paradigm?, Stanford University, February 7, 2000

*The Impact of Technology on Law and Legal Culture (Session Leader), American Association of Law Schools Mini-Workshop, Washington, D.C., January 6, 2000

*Hardware-Based ID, Rights Management, and Trusted Systems, Telecommunications Policy Research Conference, Alexandria, Virginia, September 27, 1999

*Hardware-Based ID, Rights Management, and Trusted Systems, Conference on the Commodification of Information, Haifa University Faculty of Law, May 31, 1999

*Internet Regulation, MIT Internet Telephony Consortium (semiannual meeting), Cambridge, Massachusetts, January 28, 1999

*Convergence Roundtable, hosted by the Office of Vice President Al Gore and NTIA, Washington, D.C., December 1, 1998

*The Telecommunications Act of 1996, Telecommunications Policy Research Conference, Alexandria, Virginia, October 4, 1998

*Is Internet Telephony a Regulatory Artifact?, Bellcore Internet Telephony Workshop, Washington, D.C., September 18, 1998

*Internet Connectivity, International Bar Association 1998 Conference, Vancouver, Canada, September 15, 1998

*Voice Over the Internet, a workshop sponsored by the New York State Telecommunications Association, Syracuse, New York, June 24, 1998

*Telecommunications Competition, Federal Communications Bar Association, Washington, D.C., June 16, 1998

*Colloquium on Carol M. Rose, "The Several Futures of Property — or, Of Cyberspace and Folk Tales, Emission Trades and Ecosystems" (commentor), Georgetown University Law Center, March 27, 1998

*Is Technology Really Neutral? Is PICS the Devil?, Conference on Computers, Freedom & Privacy, Austin, Texas, February 20, 1998

*Fitting Models to the Internet, AALS Section on Mass Communications Law, San Francisco, California, January 9, 1998

*Online Speech, Telecommunications Policy Research Conference, Alexandria, Virginia, September 28, 1997

*The Supreme Court and the Mass Media, University of Michigan Learning in Retirement Program, Ann Arbor, Michigan, January 9, 1997

*Reinventing Government?, C.O.B.A. [Conference of Ontario Boards and Agencies] '96, Toronto, Ontario, November 21, 1996

*A Critical Look at Internet Ratings Systems, Telecommunications Policy Research Conference, Solomons Island, Maryland, October 7, 1996

*Civil Liberties Forum, sponsored by U.S. Rep. Lynn Rivers, Wayne, Michigan, June 22, 1996

*Debating "Decency": Censorship, Free Speech, and the Internet, a conference sponsored by the Michigan Telecommunications & Technology Law Review, Ann Arbor, Michigan, April 17, 1996

*The Future of Communications Law, AALS Section on Mass Communications Law, San Antonio, Texas, January 6, 1996

*Indecency and Licensing, Symposium, Safe Harbors and Stern Warnings: FCC Regulation of Indecent Broadcasting, Villanova Law School, February 18, 1995

*Ipponka Chosei and Japan's Communications Marketplace, Federal Communications Bar Association Seminar on Doing Business in Japan, Washington, D.C., April 21, 1994

*Contradiction in Free Speech Theory, Research Group on Diversification of Media and Diversification of Regulation, at the University of Tokyo, November 18, 1992

*Administrative Guidance and Japanese Broadcast Regulation, Federal Communications Commission Office of Plans and Policy, July 28, 1992

*Perceptions of Broadcast Fairness: Broadcast Regulation in Japan and the United States, Harvard Law School East Asian Legal Studies Program, November 21, 1991. Professors Mark Ramseyer and Robert Gordon were commentators.

*Perceptions of Broadcast Fairness: Broadcast Regulation in Japan and the United States, Boston College Law School faculty colloquium, November 20, 1991

*Symposium on Freedom and Regulation in Broadcasting, University of Tokyo, June 26, 1991

*Cable Television and Copyright in the United States, Copyright Society of Japan Annual Meeting, Tokyo, June 5, 1987.

MISCELLANEOUS

*Co-chair of the Internet Corporation for Assigned Names and Numbers's Working Group C, on new generic top-level domains

*Consultant, Federal Communications Commission, 1998

*AALS Section on Mass Communications Law -- Chair, 1997; Chair-elect, 1996; Newsletter Editor, 1994-96

*Member, Advisory Board, Wayne State University Center for Legal Studies

*Court-appointed expert, Cellnet Communications v. Detroit SMSA Limited Partnership (Ameritech Mobile Communications), No. 88 CV 71292 DT (E.D. Mich.)

*Legal Editor, The American Reporter (a daily newspaper available at <http://www.american- reporter.com>), Apr.-Oct. 1995

Testimony of

Jon Weinberg

Professor of Law, Wayne State University

Detroit, MI 48202

(313) 577-3942

before the

Commission on Online Child Protection

June 8, 2000

Executive Summary

It would be untenable for the United States government simply to order the creation of a new top-level domain for material harmful to minors. Rather, if the U.S. government wishes to see such a domain created, it will have to work within the ICANN policy process. The benefits of having such a domain, though, are clouded at best. If use of the domain is not made mandatory, its mere existence will do little to reduce access by minors to sexually explicit material on the World Wide Web. But any statute purporting to make use of the domain mandatory would raise serious constitutional problems.

Prepared Testimony

Mr. Chairman and members of the Commission, I am very glad to be here today. I=m going to testify today wearing two hats. First, I=m the chair of an ICANN working group on the addition of new Internet top-level domains. Second, I=m a constitutional law professor at Wayne State University and the author of an article on Internet filtering software. I=m not speaking, though, on behalf of either ICANN, the working group or Wayne State University; rather, I=m speaking only for myself.

Background

I want to start by providing some background on the management of Internet names and addresses. Internet resources are typically identified by *domain names* such as www.copacommission.org. The domain name space is divided into top-level domains, or TLDs; each TLD is divided into second-level domains, or SLDs; and so on. Under a plan developed in 1984, there are seven Ageneric≅ three-letter top-level domains: .com, .net, .org .edu, .gov (reserved for U.S. government sites) .mil (reserved for U.S. military sites), and .int (reserved for intergovernmental organizations). In addition, there are a whole lot of two-letter Acountry code≅ top-level domains, such as .jp, .us and .fr.

When a user, looking for a particular Internet resource, types in a domain name, his computer looks to a set of local *domain name servers* that are specified within its software to find the Internet address corresponding to that domain name. Those local servers, if they don=t know the answer, will kick the problem up to a higher level. At the top of the pyramid are a set of *root servers*. Whether a top-level domain is visible in the name space is determined by whether the root servers contain an entry corresponding to that domain. If a user types in a domain name incorporating a top-level domain that the root servers he consults don=t recognize, then his computer will be unable to find any resource corresponding to that domain name.

Since 1992, the job of administering the AA≡ root server, from which all of the other root servers take their lead, has been undertaken by Network Solutions, Inc., a private company, under cooperative agreements with the National Science Foundation and the Commerce Department. Since well before NSI entered the scene, overall policy oversight of the domain name system was in the hands of Dr. Jon Postel at the University of Southern California, under a contract with the Defense Department. NSI followed the directions of Dr. Postel in maintaining, and making changes to, the root servers.

This system, however, wasn=t stable. For one thing, as the Internet became increasingly international, it was incongruous for its management to be funded by U.S. government agencies charged with overseeing scientific research projects. Other countries saw the Internet as a global resource, not subject to the narrow whims of the U.S. government, and demanded a voice in its governance. For another thing, the existing domain-name management functions had no robust management structure and no formal accountability to the Internet community.

Finally, the domain-name system was facing policy choices that were beyond the ability of the old system to resolve. Some people wanted to add many new top-level domains to the root zone; others opposed this. Some wanted the domain-name registration process to incorporate strong protection for trademark owners against the registration of names similar to their trademarks; others urged that these disputes should be left to the courts. Many people urged that other firms should be able to compete with Network Solutions in the business of registering domain names, but there was considerable argument over how this should be done. Different people suggested the creation of different new entities to help resolve these issues. These issues were thrashed out, for a period of several years, in what was sometimes called the ADNS wars.≡

The United States government took a step towards resolving these issues by midwifing the birth of a new, private, nonprofit corporation, with an internationally representative board, called ICANN X the Internet Corporation for Assigned Names and Numbers. The government announced that it would work with ICANN to transfer policy authority over the domain-name system, and specifically charged ICANN with developing policy for the addition of new top-level domains. Initially, the U.S. government proposed that even before ICANN was formed, the government should require the addition of five new top-level domains. In its final policy statement, called the White Paper, though, the government reversed that position. It concluded that it was better for ICANN to make these decisions itself, based on global input. The White Paper noted that Athe challenge of deciding policy for the addition of new domains will be formidable.≅ It expressed support for new domains, but cautioned that Ain the short run, a prudent concern for the stability of the system suggests that expansion of [top-level domains] proceed at a deliberate and controlled pace to allow for evolution of the impact of the new [top-level domains] and well-reasoned evolution of the domain space.≅

ICANN has since engaged in extensive deliberation relating to the possible creation of new top-level domains. In April, the body responsible, within ICANN, for originating policy recommendations on domain-name issues recommended to the ICANN Board that a limited number of new top-level domains be created, in the short term, in a measured and responsible manner. It referred to the possibility of introducing Afully open top-level domains, restricted and chartered top-level domains with limited scope, non-commercial domains and personal domains.≅ It cautioned, however, that there must be Aa responsible process for introducing new gTLDs, which includes ensuring that there is close coordination with organizations dealing with Internet protocols and standards.≅

It=s not at all clear that this whole process will go smoothly. ICANN is still feeling its way, and not all players in the Internet arena fully accept its authority. The U.S. government, indeed, hasn=t yet relinquished its own policy authority over the root.

Feasibility

In one sense, it would be Afeasible≅ for Congress to order, tomorrow, the addition of a top-level domain specifically intended for material harmful to minors. Both Network Solutions and ICANN are subject to U.S. jurisdiction. Congress could order Network Solutions to add the new domain to the root servers, and to host the new domain=s registry; or it could order ICANN to find a registry to host the new domain, and to request NSI to make the appropriate root server modification. Congress has the raw power to do that.

From the standpoint of the transition of domain-name policymaking authority to ICANN, though, such a move would be disastrous. ICANN is still finding its credibility as a body, independent of national governments, to govern Internet identifiers on behalf of the Internet community. For Congress to short-circuit ICANN=s processes, ordering a particular top-level domain deployed without regard to ICANN=s own choices, would strip the ICANN process of its integrity and would make it much harder for anyone to take ICANN seriously as an independent entity for Internet technical management.

Further, this would not be the end of government involvement in ICANN decision-making. Other governments would feel entitled to have their own preferences reflected in the domain name space. Other governments would come to ICANN and insist that there be top-level domains created to reflect their own policy preferences. Given the range of speech favored and disfavored by various world governments X including speech promoting Naziism or hate, speech tarnishing the Muslim religion, and so on X it is easy to imagine multiple calls by a wide range of governments for special top-level domains for speech they want to see ghettoized. Indeed, some governments would likely go farther and ask that ICANN use its own bureaucratic apparatus to enforce rules governing who could and could not register in a given domain.

This would damage the U.S. government=s effort to transfer domain-name management to a representative, bottom-up, private organization that could expand the name space while imposing minimalist rules. It could contribute to ICANN=s failure X and if ICANN fails, one likely result is a splintering of control, with the emergence of new sets of root servers not subject to U.S. authority at all. Alternatively, it could place irresistible pressures on ICANN to become a vehicle for the policy preferences of other world governments, each of them hostile to a different category of speech.

The bottom line is that if the U.S. government were to seek the creation of such a top-level domain as part of the global name space, it would be necessary to work within the ICANN process; it would be destructive to seek to impose that directive from without. Working within the ICANN process, I=ll warn you, is difficult, slow and contentious. Further, it=s not at all clear how ICANN would appropriately structure such a domain as part of a global name space. I understand that Roger Cochetti will be discussing some of the issues that would arise in that context, so I=ll not linger long on them here. Since I am a scholar of filtering and constitutional law, though, I do want to discuss some of the consequences of having this sort of top-level domain at all.

Consequences

To the extent that particular web sites are located only in a particular top-level domain, the enterprise of filtering those sites would be trivial. We would see extensive new filtering, I believe, on routers and servers. That is, if there were a .XXX domain, I expect that a substantial number of Internet service providers would choose to make resources in that domain completely unavailable to their users. Indeed, a significant number of countries would do the same. This would be sufficiently effective, in limiting the commercial reach of sites located in such a domain, that I would expect relatively few U.S.-based sites would voluntarily move there, discontinuing their presence in .com. (On the other hand, some might well move there while maintaining an identical presence in .com.) No sites based outside the U.S. would discontinue their existing sites. The upshot is that the establishment of such a domain, without more, would do little to reduce access by minors to sexually explicit material on the World Wide Web. Any value it had in facilitating filtering would likely be outweighed by its disadvantages in providing to some minors a sure-fire way of finding sexually explicit materials.

The regulatory alternative would be to make use of the domain mandatory -- that is, to make it illegal for U.S.-based speakers to distribute certain categories of speech via the World

Wide Web, except at a web site located in the particular top-level domain. This would raise substantial first amendment issues, though. As I mentioned a moment ago, a site located in such a domain would have vastly smaller reach X a substantial number of ISPs would not make it available at all. While individual users would not have to subscribe to those ISPs, a user might well find that if he wanted access to a particular site, he would have to change ISPs in order to do so. Further, any site located in that domain would immediately be branded, in the public eye, as pornography. As a result, requiring a particular speaker to locate in the Aharmful to minors≡ top-level domain would substantially interfere with his ability to get his message out.

This would, in turn, raise all of the first amendment issues that arose in the *Reno v. ACLU* and COPA litigations. How should the class of speakers to be exiled to this domain be defined? Recall the Supreme Court=s question in *Reno v. ACLU*: ACould a speaker confidently assume that a serious discussion about birth control practices, homosexuality, the First Amendment issues raised by the Appendix to our Pacifica opinion, or the consequences of prison rape would not≡ be covered by the statute? Speakers would have reason to fear, the Court continued, that a prosecutor would read the statute to extend to discussions about safe sexual practices or artistic images including nude subjects. It seems to me plain that it would be unconstitutional to require speakers like those to exile themselves, on pain of criminal prosecution, to a top-level domain from which they could not realistically be heard. That means, though, that such a statute would face the same sort of constitutional obstacles as have prior statutes in this area.

Conclusion

In sum: It would be untenable for the United States government simply to order the creation of a new top-level domain for material harmful to minors. Rather, if it wishes to see such a domain created, it will have to work within the ICANN policy process. The benefits of having such a domain, though, are clouded at best. If use of the domain is not made mandatory, its mere existence will do little to reduce access by minors to sexually explicit material on the World Wide Web. But any statute purporting to make use of the domain mandatory would raise serious constitutional problems.

I hope this testimony has been helpful. I stand ready to answer an

Senator Joe Lieberman

Now in his second term in the United States Senate, Connecticut's Joe Lieberman has earned a national reputation as a thoughtful, effective legislator. He is a Democrat who speaks his conscience, forms bipartisan coalitions with Republicans, and works for the people of Connecticut.

Lieberman connects with the concerns of a broad cross-section of the American people, which has won him respect and admiration in the Senate. He works for parents and their kids. He is pro-business. He's strong on defense. He works for the consumer and for a better environment for present and future generations.

In 1988, Lieberman won the biggest upset victory in the country by just 10,000 votes. Six years later, he made history by winning the biggest landslide victory ever in a Connecticut race for a U.S. Senate seat, with a margin of more than 350,000 votes - or 67 percent of the vote.

In endorsing his reelection in 1994, The New York Times wrote, "Congress would be a better place if more of his veteran colleagues were as good. In only one term he has influenced the course of Federal legislation for the benefit of Connecticut and the nation."

Since then, Lieberman has received praise from an increasingly wide range of observers. The Day of New London wrote, "Senator Lieberman has elevated the debate beyond partisan interests." The New York Post described him as "respected as a true man of integrity by Republicans and Democrats alike." And The Almanac of American Politics 1998 began its profile this way: "Joseph Lieberman in a decade in the Senate has exerted influence out of proportion to his seniority, committee position or political clout, an influence that came from respect for his independence of mind, civility of spirit and fidelity to causes in which he believes."

Lieberman's accomplishments include:

Defense and foreign affairs

- ensuring a strong national defense;
- promoting freedom throughout the world in places like Bosnia, China, Cuba and Eastern Europe;
- co-authoring the Gulf War Resolution;

Education

- expanding loans for small business and college students;
- backing tuition tax credits for college students and life-long learning assistance for older adults;

Environment

- strengthening Clean Air standards;

- creating Connecticut's first national park at Weir Farm;
- establishing and retaining a Long Island Sound office in the Environmental Protection Agency;
- promoting a national wildlife refuge along the Connecticut River and a "wild and scenic"status for the Farmington River;

Government reform

- strongly calling for campaign finance reform;
- exposing government waste, such as the federal contracts that paid 67 cents a page for photocopying services and $69 an hour for security guards, and the highway noise barrier projects that were built along stretches of road where nobody lived to hear the noise.
- winning passage of the Congressional Accountability Act, which makes Congress live by the same laws it applies to the nation;

Quality of Life

- strengthening the Crime Bill;
- fighting for federal enterprise zones to rebuild America's cities through the local economy;
- helping improve the Welfare reform bill with provisions to assist teenage mothers, discourage out-of-wedlock pregnancies, and help states that move Welfare recipients into self-supporting jobs.
- targeting lead poisoning, Lyme disease and indoor air pollution;

Values

- pushing the video game industry to create a rating system so parents can protect their children from violent games;
- authoring the V-Chip law, which offers parents guidance and control of television viewing by their young children.

Today, Lieberman is searching for more ways to cut middle class taxes, reform product liability laws, expand educational opportunities through charter schools and school choice, and with new legislation - The Federal Health Care Quality, Consumer Information and Protection Act (S. 795) - to improve the quality of health care.

Lieberman has cut through government red tape for tens of thousands of constituents. He enjoys staying in touch with the people of Connecticut, and has become known for his regular and popular "diner stop" visits across the state to get a taste of diners' views along with a cup of coffee.

Lieberman was born in Stamford, Connecticut on February 24, 1942 and attended public schools there. He received his bachelor's degree from Yale College in 1964 and his law degree from Yale Law School in 1967.

Lieberman was elected to the Connecticut State Senate in 1970 and served there for 10 years, including the last 6 as Majority Leader. From 1982 to 1988, he served as Connecticut's 21st Attorney General. He is the author of four books: *The Power Broker*(1966), a biography of the late Democratic Party chairman, John M. Bailey; *The Scorpion and the Tarantula* (1970), a study of early efforts to control nuclear proliferation; *The Legacy* (1981), a history of Connecticut politics from 1930-1980; and *Child Support in America* (1986), a guidebook on methods to increase the collection of child support from delinquent fathers.

In the U.S. Senate, Lieberman became the Ranking Democratic Member of the Governmental Affairs Committee in January 1999. He is a member of the powerful Armed Services Committee, the Environment and Public Works Committee, and the Small Business Committee. Since 1995, he has been Chairman of the Democratic Leadership Council.

Lieberman lives in New Haven with his wife Hadassah. They are the parents of four children: Matthew, Rebecca, Ethan and Hana. The newest arrival in the Lieberman family is granddaughter, Tennessee, born on August 13, 1997.

Prepared Testimony of Senator Joe Lieberman
COPA Commission Hearing
June 8, 2000

Mr. Chairman, I want to thank you and the other members of the Commission for providing me with an opportunity to share some of my thoughts on one of the most complicated challenges of our time – how to make the Internet both open and safe for surfers of all ages.

This is a question that in some ways the broad sweep of the electronic media in our country has been struggling with for the last several years, as standards within the entertainment industry have fallen precipitously, and as public concern has risen commensurately about the impact all of the violence, vulgarity, and degradation flooding into the public square is having on our children, our culture, and our common values.

It is also a longstanding, quintessentially American question of how to reconcile rights with responsibilities, of how to balance liberty and limits, which is to say our fundamental and at times conflicting interests in promoting free speech and free thought on the one hand and in protecting children and some semblance of social order on the other.

No one, not Madison, not Brandeis, not Brennan, has had an easy time working through this constitutional tension of freedom and community. But no matter how difficult the balancing act has been, we have always found a way to uphold these two ideals, because our democracy and the civil society undergirding it depends on both to survive. Self-government demands a free exchange of ideas and individuals willing and able to say unpopular things. But just the same, we as a national family need a common set of standards to guide us in places where the state can't and shouldn't reach. And as part of that, we need adults of all kinds, not just parents, to nurture the young morally and socially into good citizens.

That is the gist of the message I hope to communicate to you today, from my perspective both as a U.S. Senator and a parent. I know these are hard questions to answer. They are hard to answer in the analog world, and they are particularly hard in the digital one, given the uniquely open architecture of the Net and the even more open ethos of those who have cultivated its global growth. But we cannot afford to do nothing, to continue tolerating the intolerable, to continue dumping the burden solely on parents and abdicating any larger societal role in protecting our children. Not when so much is at stake, including the viability of the Internet itself.

I would urge you, in that vein, to step back and take a fresh look at what is happening on-line. The balance of rights and responsibilities that has been eroding in the old media is essentially non-existent in the new. There are practically no stop signs on the information superhighway. There are no recognizable boundaries, no common norms, no shared sense of accountability.

This digital diversity is no revelation to you or to experienced "netizens," who are well aware of the wide array of sites devoted to bombmaking, bestiality and many other expressions of antisocial behavior. These faithful users know that the Net, while offering incredible riches of information, education, and communication, has also caught just about every form of depravity known to humanity and put it on display for all the world, including our children, to see.

Yet for many parents, the anything-goes aspect of the Internet represents a threat to their ability to direct their children's upbringing, not to mention to their children's moral and physical well-being, and they are scared. A national survey done by the Annenberg Public Policy Center last year found that parents in computer households -- not the unwired – are "deeply fearful about the Web's influence on their children." Seventy-eight percent are concerned that their children will be exposed to sexually explicit material, and nearly half (49 percent) believe that their children's use of the Internet could interfere with their ability to teach values and beliefs.

The upshot is that the lack of standards has significant consequences not just for America's families, but the future of the Internet. This is something the e-commerce community understood quickly. They discovered their success online was being jeopardized by the anarchic nature of the Net and the legitimate and continuing fears people had about their personal privacy and the safety of their credit card numbers. Those threats remain, but the business world at least has acknowledged them and is formulating a response of rules. In much the same way, the Internet risks squandering the trust of America's parents, and the unparalleled potential to educate and elevate our children, if we do not find a way to draw some basic lines. In short, the Net, like any large, interactive community, can't stand long without standards.

It was in this spirit that I joined with then-Congressman Rick White two years ago in sending a letter to the nation's leading Internet companies that urged them to collaborate on a comprehensive approach to protecting children from the many different forms of harmful material they can find online. We were worried that the industry's at-that-point underwhelming efforts to safeguard young surfers would do little to mollify the very real concerns of America's parents, invite more unproductive calls for censorship, and ultimately undercut the Net's growth.

The industry answered with the launch of the GetNetWise program. On that occasion, I applauded the leaders of this project for their creativity, their sense of corporate responsibility, and in particular their sticktuitiveness, which was critical in convincing such a diverse and organizationally-challenged community to coalesce around an industry-wide solution. It was, I said, a significant step forward.

At the same time, I challenged the assembled industry leaders to avoid viewing the "one click away" program as an online bottom line, but as a portal to an ongoing effort to promote and strengthen Internet safety. It is the same challenge I make to you today. I don't know what the answer is, and I dare say neither does any one in Congress, which is why we passed a law to ask for your expertise and guidance. But I do know that ratings and icons and blocking software, all of which are helpful tools, are not enough. Technology, no matter how ingenious, is not a substitute for responsibility. There has to be some drawing of lines.

I would make three brief suggestions for you to consider. One is familiar to the old media industries, and that is to adopt a common, self-enforcing code of conduct. I know the international online community is still having trouble settling on a governing structure, let alone reaching agreement on shared standards of conduct. But if the Internet is going to continue to grow, it must self-regulate, and if it self-regulates, it must start with some basic principles.

The second is familiar to this commission and many testifying before it today and tomorrow, and that is the concept of zoning. As I understand it, you are weighing the pros and cons of creating a special domain to accommodate X-rated or other forms of adult content and segregate it away from kids. This idea, which would in effect establish a virtual red-light district, was first brought to my attention in a brilliant article written by legal commentator Jeffrey Rosen in The New Republic, which I would ask you to include in the record of your proceedings. I think this idea has a lot of merit, for rather than constricting the Net's open architecture it would capitalize on it to effectively shield children from pornography, and it would do so without encroaching on the rights of adults to have access to protected speech. In doing this, we would ask the arbiters of the Internet to simply abide by the same standard as the proprietor of an X-rated movie theater or the owner of a convenience store who sells sexually-explicit magazines.

Lastly, I would encourage you in your deliberations to look at the increasing prevalence of violent online games. I have been concerned for some time about the effect some of the more gruesome and savagely anti-social video games have on young boys. After a round of hearings that Senator Herb Kohl and I held, and some prodding on our part, the video game publishers agreed to establish an independent rating system that would warn parents about game content. That system, which I have commended on several occasions, has been in effect for six years, but I fear it is being undermined by the proliferation of independent game sites on the Web, which typically provide no ratings, no warnings of any kind to parents, and no barriers to young children to play the most hyperviolent adult-rated games. These online games can be harmful to kids, and I hope you will examine some options for limiting children's access to them.

Again, these are suggestions. I am not here to present answers. But I do know who should decide them, and that is the online community. I am very reluctant to criminalize speech or advocate any form of censorship – I was one of 16 Senators who voted against the Communications Decency Act – and I am doubtful that the U.S. Government could succeed in controlling this global medium on its own even if it tried. At the same time, I also know the risk the online community takes by doing nothing and thereby inviting Congress to pass new laws, which I believe it will do if the private sector fails to act. We can expect more court fights, more wasted time, more harm to children, and ultimately the Web will turn into a hornet's nest.

I am hopeful that we can avoid that spiral downward, and I appreciate all that this Commission is doing to find a responsible solution. Thank you again for the opportunity to testify. I look forward to your report and recommendations.â

Don't Drink! 1999 Nanny Awards Who was the most Politically Correct Person of 1999?

THE NEW REPUBLIC

March 31, 1997

ZONED OUT

by Jeffrey Rosen

Spring fever is in the air at the Supreme Court as the justices prepare to hear arguments about the constitutionality of the Communications Decency Act on March 19. To familiarize themselves with the technological obstacles to finding pornography in cyberspace, some law clerks have obtained lists of especially salacious addresses on the World Wide Web and diligently browsed at their leisure. Not since the justices gathered to watch dirty movies in the basement of the Court during the 1960s (Justice Harlan, almost blind, asked his clerks to narrate as the action unfolded) have clerkly duties been quite so arduous.

In cyberspace, too, the mood is giddy. "why we'll win" boasts the website of the Electronic Frontier Foundation; and, indeed, there is a widespread expectation that the justices, in aclu v. Reno, will agree with the three district court judges in Philadelphia who struck down the Communications Decency Act last June. But the triumphalism is premature. In light of technological and legal changes over the past year, there is now a plausible argument for upholding the constitutionality of the CDA that a majority of the Court might find convincing. In capsule form, here it is.

The CDA has two parts. The first part says, in effect, that if you display "indecent" or "patently offensive" material on the Internet, "in a manner available to a person under 18 years of age," you are a criminal. The second part says that you have a defense to prosecution if you take "reasonable, effective, and appropriate actions" to restrict access to minors, by "requiring use of a verified credit card, debit account, adult access code, or adult personal identification number."

The best argument for upholding this electronic Comstockery can be summed up in a single world: zoning. Solicitor General Walter Dellinger, in his brief, and Lawrence Lessig of the University of Chicago, in a series of powerful articles, urge us to view the CDA as an Internet zoning ordinance that channels indecent material away from children while guaranteeing full access to adults. First Amendment law recognizes three categories of sexually explicit speech: obscenity, which can be banned; ordinary speech, which must be protected; and indecency, which can be restricted for children but not for adults. In its zoning cases, the Court has said that government can move porn shops to red light districts, where children can't easily find them, or require porn sellers to check identification before selling over the counter.

In cyberspace, of course, it's much harder to discriminate on the basis of age. Users are anonymous, and teenage boys don't have to wear stilts and a mustache to disguise the fact that they are teenage boys. Just as clustering porn shops near the docks is a permissible way of discouraging crime and sloth in residential neighborhoods, the argument goes, putting porn behind electronic doors is a permissible way of ensuring that the Internet is the kind of neighborhood that parents will let their children enter in the first place.

When the three judges in Philadelphia rejected the zoning argument last June, they assumed that individual speakers on the Internet would have to set up their own adult identification sites to avoid prosecution, a prospect they found "either technologically impossible or economically prohibitive." But, since last June, the technology has changed in response to the market. Services with names like "Adult Check" and "Porno Press" now provide adult identification numbers to individual Internet users for a one-time fee of $9.95, charged to a credit card; the number then serves as a "key" that provides easy access to all the Internet sites that put up the "gates" required by the CDA. This system is no longer "economically prohibitive" for the Internet sites that use it; on the contrary, "Adult Check" actually pays the sites a fee for each user they refer.

So the age verification system doesn't appear to be an insuperable burden for porn suppliers. Is it an unconstitutional burden for adult porn consumers? The answer isn't obvious. Obtaining an adult identification number requires some effort, a minimal fee, a credit card or money order and the associated stigma of having the fee show up on your credit card bill. In the future, civil liberties organizations might set up their own adult verification sites to minimize the stigma--you could order your password from "aclu check" rather than "Adult Check"--but consumers of porn would still have to identify themselves as consumers of porn. (Today, by contrast, free samples can be downloaded anonymously from the Web and from Usenet newsgroups.) Whether the embarrassment of this act of self-identification is comparable to the embarrassment of being observed by your neighbors sneaking out of an adult bookstore is hard to say. In an adult bookstore, at least, you can wear dark glasses and pay cash to protect your anonymity. If the Court decides, in the end, that the disincentives created by the adult identification system would greatly restrict the ability of adults to buy Playboy, it should probably strike down the CDA. But, because the Internet has vastly diminished the opportunity costs associated with buying porn (you no longer need to drive from Cincinnati to Kentucky, for example), the justices might reasonably conclude that the burdens of an adult I.D. are comparatively small.

The opponents of the CDA have another argument along the same lines. An adult identification system isn't the "least restrictive means" of keeping porn out of the hands of children, they argue, because there's a less restrictive, and more effective, technology available: the Platform for Internet Content Selection, or pics. pics is a rating and filtering technology, like the V- chip, that permits content providers, or third-party interest groups, to set up their own private rating systems for any "pics-compatible" document that is posted online. Individual users can then choose the rating system that best reflects their own values, and any material that offends them will be blocked from their homes.

The aclu praises pics for allowing individual users to exercise perfect choice about what comes into their homes. Lawrence Lessig, by contrast, suggests that "pics is the devil," from a free speech perspective, because it allows censorship at any point on the chain of distribution. Countries like China or Singapore, or American corporations afraid of lawsuits, can decide what kind of speech they want to make available to their workers, and impose draconian restrictions from above. In the long run, Lessig suggests, pics will suppress more speech than an adult identification system would, because it will allow those who control access to individual terminals to filter out uncongenial ideas. But for the Supreme Court to accept this as a constitutional argument would require it to embrace a collectivist view of the First Amendment, which says that citizens should be exposed to a diversity of views, whether they want to be or not. If, on the other hand, you believe that the First Amendment is more concerned with preventing government from restricting the autonomy of individual speakers, then pics seems less intrusive than checking I.D.s.

Up until now, I've been discussing the CDA as if its language about "indecent" or "patently offensive" material, "as measured by contemporary community standards" that "depicts or describes sexual or excretory activities or organs," refers only to the kind of sexually explicit speech that the Supreme Court has said can be restricted for children. The Clinton Justice Department has tried to support this view by announcing that it will enforce the statute only against commercial pornographers. But this is hardly the most natural reading of the statute. In striking down the CDA, two of the three judges in Philadelphia held that the phrases "indecent" and "patently offensive" are unconstitutionally vague and might inhibit speech that has nothing to do with pornography, such as discussion groups about gay rights or Joyce's Ulysses.

The vagueness argument, however, is hard to sustain in light of an unfortunate Supreme Court opinion handed down on June 28, 1996, several weeks after the Philadelphia decision. Justice Stephen Breyer, joined by three of his colleagues, held that the Cable Television Consumer Protection Act, which permits cable operators to ban programming that depicts "sexual or excretory activities or organs in a patently offensive manner," is vague but not "impermissably vague." The "patently offensive" language for defining indecency, Breyer held breezily, was "similar" (although not identical) to the Supreme Court's test for defining obscenity; and Breyer concluded that Congress intended to prohibit "pictures of oral sex, bestiality and rape, and not ... scientific or educational programs (at least unless done with a highly unusual lack of concern for viewer reaction)."

The imprecision of Breyer's analysis threatens to confuse an already confused area of the law. But, in light of Breyer's holding that the government has a compelling interest in shielding children from "indecent" speech, it will be hard to argue that the identical language in the CDA is unconstitutionally vague. Opponents can try to argue that the amorphous "indecency" standard is especially inappropriate for cyberspace, where everyone is a broadcaster, but not everyone has a lawyer. (In real space, there are just a few broadcasters, and all of them have lawyers.) Moreover, the category of "indecency" was cobbled together because of the uniquely intrusive qualities of television, and on the Internet it's easier to protect children with electronic gateways. But this ends up being an argument in favor of the CDA, not against it.

Justice Breyer's indulgent view of the Cable Television Act shows the hazards of constitutional pragmatism. He criticized his colleagues for lacking the "flexibility necessary to allow government to respond to very serious practical problems," such as protecting children from indecency. But he failed to consider the degree to which the distinctions between indecency, pornography and obscenity are increasingly unstable in a global information age. Cable television and the Internet have called into question the distinction between pornography and obscenity by exposing the incoherence of geographically identifiable "community standards": especially in cyberspace, it's unrealistic to expect individual speakers to be able to predict the standards of the thousands of communities that their words and pictures may enter without their consent. It wouldn't be inconsistent with recent trends in law and technology for the Court to uphold the Communications Decency Act. It would, however, be a mistake.

(Copyright 1997, The New Republic)

Table of Contents: The New Republic 03-31-97
About The New Republic
Subscribe to The New Republic
Search the Archives
Talk to The New Republic

ENOUGH IS ENOUGH

Making The Internet Safer for Children & Families

MISSION STATEMENT

The mission of Enough Is Enough is to promote Internet safety for children and families. Our particular focus is on the twin problems of children's access to pornography and predators' access to children. We promote solutions based on separate but complimentary responsibilities between the public, technology and the law.

Enough Is Enough's activities include presenting Internet safety in schools to children, teachers and parents; promoting Codes of Ethical Conduct in the Internet industry; supporting carefully-focused legislation; and communicating the issue to the media, the public policy community and the general public.

BRUCE WATSON

Bruce Watson is the President of Enough Is Enough. Until 1996, Bruce's career was in the business world. He was a managing partner with KPMG, the international accounting and financial services firm, and subsequently served as a senior officer of a large public company. His decision to take a sabbatical from the business world to promote the issue of Internet safety reflects the growing unease felt by many parents about the environment in which we are raising our children. Bruce is married with children aged 14 and 12 respectively.

In 1998 Bruce was a lead writer of an *amicus* brief on the harms of pornography, which was cited by the Court of Appeals (District of Columbia Circuit) in the *Amatel* case. In 1999 he contributed to an *amicus* brief on the Child Online Protection Act, which is currently under review by the Third Circuit Court of Appeals. His article on "Why Libraries Should Filter Internet Access" was published in the Summer 1999 issue of the *Children's Legal Rights Journal* (Loyola University Chicago School of Law).

ENOUGH•IS•ENOUGH

Commission on Child Online Protection

Testimony by Bruce Watson
President, Enough Is Enough

June 8, 2000

I Introduction

Thank you for the opportunity to speak today in support of a separate Internet domain for material that is harmful to minors. At Enough Is Enough, we believe that such a domain can be an important part of the solution to child protection online.

Let me be clear, however, that we are not suggesting that such a domain is a "silver bullet" that would render all other parts of the solution unnecessary. The Internet is probably the most significant revolution in communications since the invention of the printing press. It would be simplistic to imagine that the issues it raises could be solved by any single panacea.

The most commonly suggested single panacea (in some quarters) is that child protection online should be left entirely to parents. Parents certainly have the primary responsibility for raising their children, and their responsibility is no less in the area of Internet safety. However, it is simply unrealistic to believe that parents can do the job alone – even if they were as Internet-literate as their children, which is frequently not the case.

By comparison, parents also have the primary responsibility to teach their children about the dangers of irresponsible use of tobacco or alcohol. But in those areas (where, incidentally, many parents have more knowledge than they do about the Internet) parents also have the support of laws making it illegal for others to provide alcohol or tobacco to their children – not to mention restrictions on even advertising such products to minors.

We believe that children's protection online similarly requires separate but complimentary responsibilities on the part of parents; other gatekeepers like teachers and librarians; the internet industry; the law and law enforcement; and, yes, maybe even the pornographers too. A separate domain would be an assist to meet these various responsibilities, not an opiate to make them go away.

II Why creating an Adult Domain deserves serious consideration

1 An adult zone will make HtM material much easier to isolate.

There is a considerable amount of misinformation and disinformation about filtering. Opponents of filtering trumpet any examples of over- or under-blocking with a glee that dramatically overstates their frequency, and sometimes suggest that all filters depend on simple word association, which is simply not true.

Nevertheless, it is certainly true that identifying all new porn sites is a significant challenge for filtering companies, whether their software operates by some form of artificial intelligence or by using so-called "spiders" to add to their proprietary database. With an adult domain, however, filtering a large portion of the troublesome material becomes instead a binary question – a "yes or no" test.

The advantage of this binary test would be to make it significantly easier to protect children from HtM material. How difficult would it be, for example, for AOL and other service providers to add "block adult domain" to their list of parental control options? The same question could presumably be added to any browser.

2 A broad-based problem needs a broad-based solution

The Internet, for all its many blessings, has also created an unprecedented, effortless and almost automatic distribution system for pornographers. It is no exaggeration to point out that it is easier for a 12-year-old to find hard-core pornography on the Internet today, than it was for an adult to find it in many American cities ten years ago. (By "hard-core" I mean what prosecutors call "penetration clearly visible," or PCV, not mere *Playboy* centerfolds.) By comparison with this effortless distribution system, solutions like filtering software and one-click-away resources require effort and expertise on the parts of parents.

While we support "one-click-away" solutions – in fact, three years ago our own website was one of the first to provide this type of help - we also recognize that, compared to the effortless reach of the distribution system, such solutions have a limited audience. Part of the solution, at least, must be coextensive with the reach of the problem – just as the limitations on selling or advertising tobacco or alcohol apply to all minors, not just those whose parents best understand the problem.

3 Zoning is what we already do in the physical world

The right objective for Cyberspace with respect to HtM material should be for it to be subject to the same standards as the physical world - neither more nor less. Our society accepts that certain material is acceptable for adults but not for kids; as illustrated, for example, by the zoning of sexually-oriented businesses that are for adults only, or the use of blinder racks for adult magazines in newsstands. A "dot adult" Internet zone recognizes the same reality. Why would we not apply the same concept to cyberspace?

III – Questions and Answers

1 Would an adult domain create an attractive nuisance that would make it easier for children to find HtM materials?

Unfortunately, lest we forget, it would be just about impossible for pornography to be easier to find on the Internet than it already is. I have attached the Enough Is Enough fact sheet "Is Pornography Really So Easy To Find On The Internet?" for the record. If a person is looking for pornography on the Internet, it is already almost impossible to miss.

The words "sex" and "porn" are consistently at or near the top of the list of words entered into search engines, and lead quickly to free samples of hard-core material. In other words, the attractive nuisance already exists. With an adult domain, however, the attractive nuisance would at least be easier to isolate.

2 If U.S. law required use of the domain, would this lead HtM sites to move offshore?

The answer to this question has a number of parts. Firstly, if a U.S. corporation or individual placed a porn web site offshore, it is not self-evident that they would necessarily escape U.S. jurisdiction - any more than the person who opens an offshore bank account necessarily avoids IRS jurisdiction over the interest income. It is interesting to note that England has already prosecuted an English porn site operator who located his site here in the U.S. in the vain hope of escaping English jurisdiction.

Secondly, the U.S. is not the only country troubled by this issue, which is under serious study with varying legislative proposals in the European Union, Australia and other countries. Between shared concerns and moral suasion, the number of potential havens could be expected to drop with the passage of time. Already, in the battle against child pornography, there is a notable amount of international cooperation - for example, the roundup of the "Wonderland" child pornography ring, which involved simultaneous arrests in twelve countries.

The U.S. has been the leader in developing the Internet. Should we not also be the leader in developing solutions to the problems it has brought with it?

3 Would creating an adult domain effectively legalize obscenity?

Creating an adult domain for HtM material would not legitimize obscenity any more than creating a sexually-oriented business zone does in the physical world. In neither case does the decision to create an adult zone imply that obscene materials will be or should be free from prosecution.

Another advantage of an adult domain, however, is that it would aid in shielding children from the large amount of unprosecuted obscenity already present in U.S. web sites on the Internet. At a recent public hearing of the House Commerce Committee here in Washington, representatives of the Justice Department confirmed – albeit grudgingly - that they have initiated almost no prosecutions of Internet obscenity in the last five years. While this lack of energy by the Justice Department is a scandal in itself, an adult domain would at least provide some level of safety net between children and any unprosecuted obscenity on the Internet.

4 Should it be mandatory for porn sites to reside in the adult domain?

In an ideal world, it would not be necessary to make compliance mandatory. In fact, ideally porn sites would already have taken voluntary steps to keep their materials from younger eyes. Instead, however, we find the opposite - "stealth" porn sites using child-appeal brand names like Disney, Pokemon, or Barbie to bring traffic to their sites.

It is obviously unlikely that the owners of such sites would voluntarily relocate to an adult domain, since, for whatever reason, advertising to children appears already to be part of their standard operating procedure. The use of an adult domain by HtM sites should, therefore, be made mandatory.

5 Is it possible to adequately define which materials should be in this domain?

It's interesting that this question causes more trouble to well-meaning academics than it does to commercial pornographers, who know exactly what will sell – and it's not Michaelangelo's *David* or AIDS prevention information. The guy running the Pink Kitty Porn Palace isn't showing video tours of the Louvre! The idea that it is beyond human capacity to define in words what the porn merchants can tell at a glance is, well, improbable.

Those whose interests or ideology are advanced by making pornography as widely available as possible like to focus attention on the borderline cases – say, AIDS prevention sites or gynecology sites – suggesting that the mere existence of marginal cases makes any law automatically vague and unenforceable. This is the only area of law, however, where anyone seriously suggests that the existence of marginal cases makes the entire objective unattainable. In defending a manslaughter charge, the borderline difference between "self-defense" and "provocation" can be the difference between jail time and freedom. Should we abandon the law of manslaughter because juries have to make judgment calls?

While a number of different approaches could be taken to defining the reach of an adult domain, it is unreasonable to suggest that it is beyond definition. And the harsh reality is that there is a host of material already on the Internet that is harmful to minors by almost any standard.

ENOUGH•IS•ENOUGH

Commission on Child Online Protection

Testimony by Bruce Watson
President, Enough Is Enough

June 8, 2000

I Introduction

Thank you for the opportunity to speak today in support of a separate Internet domain for material that is harmful to minors. At Enough Is Enough, we believe that such a domain can be an important part of the solution to child protection online.

Let me be clear, however, that we are not suggesting that such a domain is a "silver bullet" that would render all other parts of the solution unnecessary. The Internet is probably the most significant revolution in communications since the invention of the printing press. It would be simplistic to imagine that the issues it raises could be solved by any single panacea.

The most commonly suggested single panacea (in some quarters) is that child protection online should be left entirely to parents. Parents certainly have the primary responsibility for raising their children, and their responsibility is no less in the area of Internet safety. However, it is simply unrealistic to believe that parents can do the job alone – even if they were as Internet-literate as their children, which is frequently not the case.

By comparison, parents also have the primary responsibility to teach their children about the dangers of irresponsible use of tobacco or alcohol. But in those areas (where, incidentally, many parents have more knowledge than they do about the Internet) parents also have the support of laws making it illegal for others to provide alcohol or tobacco to their children – not to mention restrictions on even advertising such products to minors.

We believe that children's protection online similarly requires separate but complimentary responsibilities on the part of parents; other gatekeepers like teachers and librarians; the internet industry; the law and law enforcement; and, yes, maybe even the pornographers too. A separate domain would be an assist to meet these various responsibilities, not an opiate to make them go away.

II Why creating an Adult Domain deserves serious consideration

1 An adult zone will make HtM material much easier to isolate.

There is a considerable amount of misinformation and disinformation about filtering. Opponents of filtering trumpet any examples of over- or under-blocking with a glee that dramatically overstates their frequency, and sometimes suggest that all filters depend on simple word association, which is simply not true.

Nevertheless, it is certainly true that identifying all new porn sites is a significant challenge for filtering companies, whether their software operates by some form of artificial intelligence or by using so-called "spiders" to add to their proprietary database. With an adult domain, however, filtering a large portion of the troublesome material becomes instead a binary question – a "yes or no" test.

The advantage of this binary test would be to make it significantly easier to protect children from HtM material. How difficult would it be, for example, for AOL and other service providers to add "block adult domain" to their list of parental control options? The same question could presumably be added to any browser.

2 A broad-based problem needs a broad-based solution

The Internet, for all its many blessings, has also created an unprecedented, effortless and almost automatic distribution system for pornographers. It is no exaggeration to point out that it is easier for a 12-year-old to find hard-core pornography on the Internet today, than it was for an adult to find it in many American cities ten years ago. (By "hard-core" I mean what prosecutors call "penetration clearly visible," or PCV, not mere *Playboy* centerfolds.) By comparison with this effortless distribution system, solutions like filtering software and one-click-away resources require effort and expertise on the parts of parents.

While we support "one-click-away" solutions – in fact, three years ago our own website was one of the first to provide this type of help - we also recognize that, compared to the effortless reach of the distribution system, such solutions have a limited audience. Part of the solution, at least, must be coextensive with the reach of the problem – just as the limitations on selling or advertising tobacco or alcohol apply to all minors, not just those whose parents best understand the problem.

3 Zoning is what we already do in the physical world

The right objective for Cyberspace with respect to HtM material should be for it to be subject to the same standards as the physical world - neither more nor less. Our society accepts that certain material is acceptable for adults but not for kids; as illustrated, for example, by the zoning of sexually-oriented businesses that are for adults only, or the use of blinder racks for adult magazines in newsstands. A "dot adult" Internet zone recognizes the same reality. Why would we not apply the same concept to cyberspace?

III – Questions and Answers

1 Would an adult domain create an attractive nuisance that would make it easier for children to find HtM materials?

Unfortunately, lest we forget, it would be just about impossible for pornography to be easier to find on the Internet than it already is. I have attached the Enough Is Enough fact sheet "Is Pornography Really So Easy To Find On The Internet?" for the record. If a person is looking for pornography on the Internet, it is already almost impossible to miss.

The words "sex" and "porn" are consistently at or near the top of the list of words entered into search engines, and lead quickly to free samples of hard-core material. In other words, the attractive nuisance already exists. With an adult domain, however, the attractive nuisance would at least be easier to isolate.

2 If U.S. law required use of the domain, would this lead HtM sites to move offshore?

The answer to this question has a number of parts. Firstly, if a U.S. corporation or individual placed a porn web site offshore, it is not self-evident that they would necessarily escape U.S. jurisdiction - any more than the person who opens an offshore bank account necessarily avoids IRS jurisdiction over the interest income. It is interesting to note that England has already prosecuted an English porn site operator who located his site here in the U.S. in the vain hope of escaping English jurisdiction.

Secondly, the U.S. is not the only country troubled by this issue, which is under serious study with varying legislative proposals in the European Union, Australia and other countries. Between shared concerns and moral suasion, the number of potential havens could be expected to drop with the passage of time. Already, in the battle against child pornography, there is a notable amount of international cooperation - for example, the roundup of the "Wonderland" child pornography ring, which involved simultaneous arrests in twelve countries.

The U.S. has been the leader in developing the Internet. Should we not also be the leader in developing solutions to the problems it has brought with it?

3 Would creating an adult domain effectively legalize obscenity?

Creating an adult domain for HtM material would not legitimize obscenity any more than creating a sexually-oriented business zone does in the physical world. In neither case does the decision to create an adult zone imply that obscene materials will be or should be free from prosecution.

Another advantage of an adult domain, however, is that it would aid in shielding children from the large amount of unprosecuted obscenity already present in U.S. web sites on the Internet. At a recent public hearing of the House Commerce Committee here in Washington, representatives of the Justice Department confirmed – albeit grudgingly - that they have initiated almost no prosecutions of Internet obscenity in the last five years. While this lack of energy by the Justice Department is a scandal in itself, an adult domain would at least provide some level of safety net between children and any unprosecuted obscenity on the Internet.

4 Should it be mandatory for porn sites to reside in the adult domain?

In an ideal world, it would not be necessary to make compliance mandatory. In fact, ideally porn sites would already have taken voluntary steps to keep their materials from younger eyes. Instead, however, we find the opposite - "stealth" porn sites using child-appeal brand names like Disney, Pokemon, or Barbie to bring traffic to their sites.

It is obviously unlikely that the owners of such sites would voluntarily relocate to an adult domain, since, for whatever reason, advertising to children appears already to be part of their standard operating procedure. The use of an adult domain by HtM sites should, therefore, be made mandatory.

5 Is it possible to adequately define which materials should be in this domain?

It's interesting that this question causes more trouble to well-meaning academics than it does to commercial pornographers, who know exactly what will sell – and it's not Michaelangelo's *David* or AIDS prevention information. The guy running the Pink Kitty Porn Palace isn't showing video tours of the Louvre! The idea that it is beyond human capacity to define in words what the porn merchants can tell at a glance is, well, improbable.

Those whose interests or ideology are advanced by making pornography as widely available as possible like to focus attention on the borderline cases – say, AIDS prevention sites or gynecology sites – suggesting that the mere existence of marginal cases makes any law automatically vague and unenforceable. This is the only area of law, however, where anyone seriously suggests that the existence of marginal cases makes the entire objective unattainable. In defending a manslaughter charge, the borderline difference between "self-defense" and "provocation" can be the difference between jail time and freedom. Should we abandon the law of manslaughter because juries have to make judgment calls?

While a number of different approaches could be taken to defining the reach of an adult domain, it is unreasonable to suggest that it is beyond definition. And the harsh reality is that there is a host of material already on the Internet that is harmful to minors by almost any standard.

ENOUGH•IS•ENOUGH

Is Pornography Really So Easy to Find on the Internet?

Many people wonder how easy pornography is to find on the Internet, since there is a great deal of misinformation on the subject. Unfortunately, pornography is freely and easily available to children on the Internet, in both commercial areas on the World Wide Web and in non-commercial areas such as Usenet newsgroups.

In addition to pornography which would be considered legal for adults in print and broadcast media, children have access on the Internet to material which is illegal even for adults, such as obscenity and child pornography. Even worse, children can find this material intentionally or unintentionally.

Unintentional access to pornography

1. Stealth sites: There are numerous hard-core pornography sites on the Internet using "copycat URLs" to take advantage of innocent mistakes to bring traffic to their graphic sexual images.
    a) Mirror sites: Children searching the Internet for the official web site of the White House can be confronted by hard-core pornography by mistyping www.whitehouse.com, rather than whitehouse.gov. The official NASA site has been similarly copied by pornographers.
    b) Spelling errors: Children who mistype www.betscape.com instead of netscape.com, or www.sharware.com instead of shareware.com, will be confronted with live sex shows and other X-rated pictures.
    c) Misuse of brand name: A key word search for "amazon.com" also yields links to the porn index "amazon-cum.com." An innocent search on "Disney cartoons" can yield links to hard-core pornographic cartoons.
2. Key word search: Children using Internet search engines to look up innocent information will easily receive links to pornographic sites:
    a) Innocent searches for toys, dollhouse, girls, boys, or pets can yield numerous links to sexually explicit sites, like www.boys.com, which features men and boys engaged in sexual activity.
    b) Even more disturbing, searches on children's favorites like Nintendo characters (such as Pokemon) can lead to porn locations. Are these hard-core porn sites deliberately targeting children?

Intentional access to pornography

Curiosity in children and teenagers is natural and healthy, but if you seek pornography on the Internet, it is almost impossible to miss. Youngsters seeking information about sexuality on the Internet will be confronted with pornography's negative, anti-social messages that can forever alter their views of sexuality and relationships.

1. Key word search: Curious children and teenagers can easily find pornography using search engines and words like "sex", "hard-core", and similar terms.
2. Obvious URLs: Children and teenagers can guess at explicit web addresses such as www.sex.com and even www.bestiality.com and view graphic hard-core pornography.

Once children have been exposed to graphic sexual content on the Internet, their innocence can never be regained. The protection of children from pornography should not be entirely up to their own self-discipline.

Robert Corn-Revere

Mr. Corn-Revere is a partner in the Washington, D.C. office of Hogan & Hartson L.L.P., concentrating in First Amendment, Internet and communications law. He regularly advises clients on FCC and Internet-related issues and has served as counsel in First Amendment litigation involving the Communications Decency Act, the Child Online Protection Act, Internet content filtering in public libraries and export controls on encryption software. In 1999, Mr. Corn-Revere was listed on a 30th Anniversary Roll of Honor by the American Library Association Office of Intellectual Freedom and Freedom to Read Foundation for his role as lead counsel in *Mainstream Loudoun v. Board of Trustees of the Loudoun County Library*.

Before joining Hogan & Hartson in 1994, Mr. Corn-Revere served as Chief Counsel to Interim Chairman James H. Quello of the Federal Communications Commission. Previously, from 1990 until 1993, he was Commissioner Quello's Legal Advisor. Before entering government service, Mr. Corn-Revere was an associate at Hogan & Hartson from 1985 to 1990, and at another Washington D.C. firm from 1983 to 1985.

Since 1987, Mr. Corn-Revere has taught at the Communications Law Institute of the Columbus School of Law, Catholic University of America. He currently teaches a seminar in First Amendment law, and is faculty advisor to CommLaw Conspectus, a journal of communications law and policy. He is Chairman of the Media Institute's First Amendment Advisory Council and is a member of the Institute's Board of Trustees. Mr. Corn-Revere is also an Adjunct Scholar to the Cato Institute and to Citizens for a Sound Economy Foundation in Washington D.C.

Mr. Corn-Revere has written extensively on First Amendment, Internet and communications-related issues and is a frequent speaker at professional conferences. He is co-author of a three-volume treatise entitled, "Modern Communications Law," published by the West Group in 1999. In addition, Mr. Corn-Revere serves on the Editorial Advisory Board of Pike & Fischer's Internet Law & Regulation, the Editorial Board of Commercial Speech Digest and the Board of Advisors of the Online Ombuds Office of the University of Massachusetts Center for Information Technology and Dispute Resolution. In the past Mr. Corn-Revere worked as a journalist, both for daily newspapers, and for magazines as a freelance writer.

Mr. Corn-Revere received his J.D. from the Columbus School of Law in 1983, where he was Lead Articles Editor of the Catholic University Law Review. He earned an M.A. from the University of Massachusetts-Amherst in 1980 and a B.A. from Eastern Illinois University in 1977. Mr. Corn-Revere is a member of the District of Columbia Bar, as well as the United States Supreme Court, District of Columbia, Third, Fourth, and Eleventh Circuit Bar

Testimony of Robert Corn-Revere

Before the

COPA Commission

Legal and Policy Implications of "Cyberzoning"

June 8, 2000

Robert Corn-Revere
Hogan & Hartson L.L.P.
Columbia Square
555 13th Street, N.W.
Washington, D.C. 20004
(202) 637-5600
cornrevere@hhlaw.com

Mr. Corn-Revere is a partner in the Washington, D.C. office of Hogan & Hartson L.L.P., specializing in First Amendment, Internet and communications law. Before joining Hogan & Hartson in 1994, Mr. Corn-Revere served as Chief Counsel to Interim Chairman James H. Quello of the Federal Communications Commission. Previously, from 1990 until 1993, he was Commissioner Quello's Legal Advisor. Before entering government service, Mr. Corn-Revere was an associate at Hogan & Hartson from 1985 to 1990, and at Steptoe & Johnson from 1983 to 1985.

Mr. Corn-Revere has written extensively on First Amendment, Internet and communications-related issues and is a frequent speaker at professional conferences. He is co-author of a three-volume treatise entitled MODERN COMMUNICATIONS LAW, published by West Publishing Company, and is Editor and co-author of the book, RATIONALES & RATIONALIZATIONS, published in 1997. He is a member of the Editorial Advisory Boards of Pike & Fischer's INTERNET LAW & REGULATION and the Media Institute's COMMERCIAL SPEECH DIGEST. Since 1987, Mr. Corn-Revere has taught at the Communications Law Institute of the Columbus School of Law, Catholic University of America. He is Chairman of the Media Institute's First Amendment Advisory Council and is a member of the Institute's Board of Trustees. Mr. Corn-Revere is also an Adjunct Scholar to the Cato Institute and to Citizens for a Sound Economy Foundation in Washington D.C. In May 2000, he was elected to the Board of Trustees of the Freedom to Read Foundation.

Testimony of Robert Corn-Revere
COPA Commission
June 8, 2000

Mr. Chairman and Members of the Commission. Thank you for this opportunity to address the significant issues that you are charged with investigating. My testimony reflects only my own views on the issues; I am not testifying on behalf of any organization or client.

I have been asked to discuss the legal and policy implications of "cyberzoning." By this term I mean the creation of designated zones on the Internet for the labeling and possible segregation of "adult" material. One potential mechanism for such zoning would be the creation of a new top level domain ("TLD") in order to provide a distinctive Internet address for specified types of sexually-oriented materials (*e.g.*, ".xxx," ".sex" or ".adult") as opposed to the familiar .com, .net and .org generic domains. This is viewed by some as a less restrictive way of preventing access by children to sexually-oriented materials than the use of direct penalties for the display or transmission of such materials.

As I explain below, such proposals frequently are more complicated than they seem at first glance, especially with respect to speech on the

Internet. While it may be tempting to apply the concept of real world zoning metaphorically to online speech, there are fundamental differences between the types of "zoning" envisioned for these distinct spaces, both in terms of the purposes to be served and in their operation and effect. In addition, there are practical difficulties associated with the use of the global domain name system as an instrument of domestic policy.

I. BACKGROUND

In 1997 the Supreme Court invalidated key portions of the Communications Decency Act, the federal government's first attempt to regulate "indecent" speech on the Internet. Reno v. ACLU 521 U.S. 844 (1997). In doing so, the Court identified the ways in which the Internet is fundamentally different from previous mass media. It described the Internet is a unique and wholly new medium of worldwide human communication that is located in no particular geographical location and has no centralized control point; a medium that is available to anyone, anywhere in the world with access. Accordingly, the Supreme Court found that the information available on the Internet is as "diverse as human thought.Id. at 850-852.

Although the Court was unanimous in striking down on First Amendment grounds those provisions of the CDA that prohibited the "display" of "indecent" materials, Justice O'Conner, joined by Chief Justice Rehnquist, dissented in part and suggested that certain methods of segregating adult materials might be permissible. They described the CDA as an attempt to "create 'adult zones' on the Internet" and suggested that future laws might survive constitutional review so long as they do not "stray from the blueprint our prior cases have developed for constructing a 'zoning law.'"Id. at 886 (O'Connor, J., concurring in part and dissenting in part). Noting that the Court previously addressed only laws that operate in the physical world, Justice O'Connor observed that "[c]yberspace is malleable" and that "it is possible to construct barriers in cyberspace and use them to screen for identity, making cyberspace more like the physical world and, consequently, more amenable to zoning laws." Id. at 890. The dissenting Justices recognized that the technology for such zoning was at an early stage of development but described the necessary preconditions for its effectiveness: (1) a uniform code for designating content, and (2) widely available (and widely used) technology that could recognize the code and restrict access for certain usersId. at 891.

Congress attempted to correct the constitutional deficiencies of the CDA when it adopted the Child Online Protection Act ("COPA"), codified at 47 U.S.C. § 231. The stated purpose of the law was to restrict the availability to children of "harmful to minors" material on commercial websites. However, for reasons that echo the Supreme Court's decision in *Reno v. ACLU*, enforcement of COPA has been enjoined by the United States District Court for the Eastern District of Pennsylvania. *ACLU v. Reno*, 31 F. Supp.2d 473 (E.D. Pa. 1999). Appeal of that decision currently is pending in the United States Court of Appeals for the Third Circuit.

During the legislative debates that led to the passage of COPA, Congress considered – and rejected – a number of zoning techniques designed to "effectively place[] the seller of pornography in a red-light district in cyberspace." H. Rep. 105-775, 105th Cong., 2d Sess. 17-20 (Oct. 5, 1998) ("HOUSE REPORT"). The analysis included such methods as tagging websites, voluntary rating systems, blocking or filtering technologies and domain name zoning. Generally, these alternatives were not embraced because it was believed that they would not protect children adequately while raising "a host of additional issues that jeopardize their success and effectiveness." *Id.* at 17.

According to the congressional analysis, a scheme of mandatory tagging or rating "would raise additional First Amendment issues because entities such as online newspapers could be asked to rate their content." *Id.* at 18. In addition, the House Report concluded that such zoning methods would be ineffective unless they were combined with some form of blocking or filtering technology. It pointed out that without the use of technology to restrict access, such methods "could actually help a minor find adult material."Id. at 18. With respect to domain name zoning, the House Report concluded that simply creating an adult domain without mandating uniform blocking techniques would be ineffective. In addition, it noted that changes in the DNS "will have international consequences" and it suggested that "the United States should not act without reaching broad industry and international consensus." Moreover, Congress expressed its reluctance "to begin regulating the computer industry." Id.

Following judicial prohibition on the enforcement of COPA, it has been suggested that new legislative proposals to mandate some form of cyberzoning might be introduced. So far as I am aware, none of the zoning measures has yet materialized, so it is not possible to address specific proposals at this time. However, there has been some discussion of various cyberzoning approaches by academic writers that provide some basis for analysis. 1/

1/ E.g., Lawrence Lessig, CODE AND OTHER LAWS OF CYBERSPACE 173-182 (Basic Books: New York 1999) ("CODE AND OTHER LAWS"); Lawrence Lessig, G-

Professor Lawrence Lessig, for example, has written that technology permits Internet browsers to be configured for individual users, so that minors could be restricted to what he describes as "G-rated surfing." To accomplish this, however, inappropriate materials would be excluded "only if servers cooperated," so that it would be necessary to adopt what he describes as "a simple law", which would provide that "[i]f a client signals gSurfing, then a server may not transmit material 'harmful to minors.'2/ Lessig explains that "with zoning, people are filtered; with filtering, the listener zones speech," and he asserts that zoning based on identifying children and excluding them from "Ginsberg speech" would be constitutional. See CODE AND OTHER LAWS, supra note 1 at 176.

To accomplish this objective at the client level may involve the government "requiring browser manufacturers to modify their browsers to permit users to set up profiles" which would include a check-off box for the user

---

Rated Browsers, THE STANDARD, Dec. 3, 1999 ("G-Rated Browsers") (http://www.thestandard.com/article/display/0,1151,8035,00.html); April Mara Major, Internet Red Light Districts: A Domain Name Proposal for Regulatory Zoning of Obscene Content, 16 John Marshall J. Computer & Info. 21, 30 (1997) ("A Domain Name Proposal for Regulatory Zoning").

2/ See G-Rated Browsers. The "harm to minors" standard refers to the variable obscenity test articulated by the Supreme Court in Ginsberg v. New York, 390 U.S. 629 (1968), which is described more fully below.

to signal he is a minor. If this box is checked on a given machine, "the other profiles on the machine would require a password." Id. When such a browser is used to surf the web, the "kid ID" would be transmitted when an attempt is made to access a web site. To be effective, "[t]his scheme would require that the web site block Ginsberg speech to any self-identified minor." Id.

On the content side, this proposal "requires those who have zonable speech to place that speech behind walls." Id. Accordingly, under Lessig's suggested "simple law," certain designated speakers on the Internet "are zoned into a space from which children are excluded." Id. at 175. One possible "space" to which Ginsberg speech" could be relegated under such a plan, would be a separate, restricted TLD under the domain name system. In this regard, the House Report on COPA noted that "there are no technical barriers to creating an adult domain, and it would be very easy to block all websites within an adult domain." House Report at 18.

II. LEGAL ANALYSIS OF CYBERZONING

The typical legal analyses of the various cyberzoning proposals attempt to apply First Amendment concepts developed in tangible space to cyberspace. On one level, this makes good sense, in that traditional legal principles are applicable to speech on the Internet. As the Supreme Court established in Reno v. ACLU, 521 U.S. at 870, there is "no basis for qualifying the level of First Amendment scrutiny that should be applied to this medium." But where efforts to place certain types of speech "behind walls" are based on legal theories built on particular physical or geographical assumptions, the analogy breaks down. In a nutshell, cyberzoning is a very different thing than zoning in real space.

A. Zoning "Adult" Businesses

The most obvious - and least appropriate - analogy is to compare cyberzoning to restrictions placed on certain types of adult businesses in the physical world. Zoning restrictions may impose certain requirements on such businesses, such as limiting their location in a community or hours of operation, just as most businesses must comply with land use requirements in physical space. For businesses that are engaged in expressive activities, certain special zoning requirements have been approved by the courts where the restrictions are designed to address "secondary effects" that may be associated with the business, including crime, prostitution, urban blight or similar problems. This "secondary effects" theory is derived from a series of cases involving the zoning of adult bookstores, movie theaters and night clubs. 3/

In defending the CDA the federal government argued that restrictions on Internet speech could be upheld under this theory. The Solicitor General's brief to the Supreme Court in Reno v. ACLU took the position that indecent speech may be regulated as if it were a "secondary effect," and the CDA's restrictions may be characterized as content-neutral "cyberzoning." Similarly, Professor April Major has suggested that Internet zoning using the DNS could be supported using a "secondary effects" analysis. The "secondary effect" to be addressed by such regulation would be the possibility that the Internet may "lose legitimacy" as a "communication and information medium" absent adult "zones." See A Domain Name Proposal for Regulatory Zoning supra note 1.

Such analyses misapprehend the meaning of the secondary effects theory. Secondary effects, by definition, are physical effects. A Renton-type analysis can apply only to real space because it is predicated on combating physical problems that may be associated with certain businesses. In this

---

3/ E.g., City of Erie v. Pap's A.M., 120 S. Ct. 1382 (2000); City of Renton v. Playtime Theatres, Inc., 475 U.S. 41 (1986); Young v. American Mini Theatres, respect, the Supreme Court has held repeatedly that Renton "secondary effects" analysis does not apply where regulation of adult businesses is based on "the content of the films being shown inside the theaters."[4] As the Supreme Court very recently reaffirmed in United States v. Playboy Entertainment Group, Inc, 2000 WL 646196 *8 (May 22, 2000), zoning cases are irrelevant to content-based regulations of speech because "the lesser scrutiny afforded regulations targeting the secondary effects of crime or declining property values has no application to content-based regulations targeting the primary effects of protected speech."

Any effort to "zone" information on the Internet can only be understood as a decision to restrict material because of its content, for there is no physical presence in cyberspace. Accordingly, the Supreme Court foreclosed the use of a "secondary effects" analysis for Internet speech in Reno v. ACLU. It held that efforts to limit access by children to "indecent" speech were based

---

Inc., 427 U.S. 50 (1976).

[4] Boos v. Barry, 485 U.S. 312, 320-321 (1988) ("Regulations that focus on the direct impact of speech on its audience . . . are not the type of 'secondary effects' we referred to in Renton."); Forsyth County v. Nationalist Movement, 505 U.S. 123, 134-136 (1992). See also Erznoznik v. City of Jacksonville, 422 U.S. 205, 214-215 (1975); Schneider v. New Jersey, 308 U.S. 147, 162-163 (1939).

on concern about the "primary effects" of that speech, rather than the secondary effects, and that any restrictions "cannot be 'properly analyzed as a form of time, place, and manner regulation.'"Reno v. ACLU 521 U.S. at 868. And the Court brushed aside as "singularly unpersuasive" the suggestion that the Internet was subject to regulation on the theory that sexually-oriented material would cause the medium to lose legitimacyId. at 885 ("The dramatic expansion of this new marketplace of ideas contradicts the factual basis of this contention."). From the perspective constitutional law, real world zoning is a metaphor that simply is inapplicable to cyberspace.

B. Regulating "Ginsberg Speech"

Another approach is to zone speech considered "harmful to minors" on the Internet in order to enable browsers to block access to such speech by children. According to Professor Lessig, this would require content providers on the Internet to designate what he calls Ginsberg speech" with code that would be read by browsers enabled with a "kids ID." This would entail passage of what is described as a "simple law" requiring the segregation of proscribed material. As I explain below, however, such a "simple law" in theory would be far from simple to implement in practice. Leaving aside any technical questions that undoubtedly would arise from enabling (or forcing) parents to use password-protected browsers with multiple "personalities," the problem of identifying and zoning "Ginsberg speech" would be highly problematic. Speaking as a former FCC official who often was required to evaluate the content of broadcast speech, I can tell you that it is not possible to neatly categorize "zonable speech," as if our task was to separate red stones from blue stones from a common pile, and to tell our children that they mustn't touch the red stones. This is particularly true if the goal is to place certain types of speech on the Internet "behind walls."

The "harm to minors" standard articulated in Ginsberg v. New York at least has the virtue of being more analytically rigorous than the indecency standard that was thoroughly deconstructed by the Supreme Court in Reno. Generally, courts have limited regulation in this area to "borderline obscenity" or to material considered to be "virtually obscene." Virginia v. American Booksellers Assn, 484 U.S. 383, 390 (1988). In order to be harmful to minors, the material must lack serious literary, artistic, political or scientific value for "a legitimate minority of normal, older adolescents."American Booksellers Assn. v. Virginia, 882 F.2d 125, 127 (4th Cir. 1989). Thus, as a general matter "if any reasonable minor, including a seventeen-year-old, would find serious value, the material is not harmful to minors.'5/ If applied strictly, this constitutional standard decreases the range of material that could be considered harmful to minors. 6/

But it must be kept in mind that any "harm to minors" test necessarily is based on local community standards. As the Supreme Court stated when it adopted the "community standards" test in Miller v. California, 413 U.S. 15, 20, 30-33 (1973), "[p]eople in different States vary in their tastes and attitudes, and this diversity is not to be strangled by the absolutism of imposed uniformity. . . .[O]ur nation is simply too big and too diverse for this Court to reasonably expect that such standards could be articulated for all 50

5/ American Booksellers v. Webb, 919 F.2d 1493, 1504-05 (11th Cir. 1990); Davis-Kidd Booksellers, Inc.v. McWherter, 866 S.W.2d 520, 528 (Tenn. 1993).

6/ Webb, 919 F.2d at 1504-05. See Rushia v. Town of Ashburnham, 582 F. Supp. 900 (D. Mass 1983) (town bylaw not sufficiently limited); American Booksellers Ass'n. v. McAuliffe, 533 F. Supp. 50 (N.D. Ga. 1981) (statute prohibiting sale or display to minors of material containing nude figures held overbroad); Allied Artists Pictures Corp.v. Alford, 410 F. Supp. 1348 (W.D. Tenn. 1976) (ordinance prohibiting exposing juveniles to offensive language held invalid); American Booksellers Ass'n.v. Superior Court, 129 Cal. App. 3d 197, 181 Cal. Rptr. 33 (2d Dist. 1982) (photographs with a primary purpose of causing sexual arousal held not to be harmful to minors); Calderon v. City of Buffalo, 61 A.D.2d 323, 402 N.Y.S.2d 685 (1978) (ordinance restricting sales to juveniles held to be overbroad); Oregon v. Frink, 60 Or. App. 209, 653 P.2d 553 (1982) (statute prohibiting dissemination of nudity to minors is overly broad).

states in a single formulation, assuming the prerequisite consensus exists." Professor Lessig notes that "Ginsberg speech" is defined by "[l]aws in many jurisdictions," CODE AND OTHER LAWS, supra note 1 at 173, evidently without acknowledging the import of that observation.

The significance of this point is that, for purposes of information on the Internet, "Ginsberg speech" is not a single standard. It is not surprising then, that different communities will have very different views on what information might be deemed "harmful to minors." For example, an Ohio court held that the books One Flew Over the Cuckoo's Nest and Manchild in the Promised Land violated the state "harmful to juveniles" law. Grosser v. Woollett, 341 N.E.2d 356, 360-361 (Ohio Ct. Common Pleas 1974).7/ The court found that the books "have no literary, artistic, political or scientific value whatsoever" and "were designed by the authors to appeal to the base instincts of persons and to shock others for the purpose of effectuating sales." Id. at 367. The dissenters in Reno v. ACLU foreshadowed such differing standards, observing that "discussions about prison rape or nude art . . . may have some

---

7/ Although this decision was issued before the Supreme Court addressed the "harm to minors" standard in American Booksellers Association, the Ohio legislature cited Grosser v. Woollett as an appropriate source of guidance when it was considering passage of new Internet regulations in 1998.

redeeming education value for adults, they do not necessarily have any such value for minors." 521 U.S. at 896 (O'Connor, J., concurring part, dissenting in part).

Nevertheless, federal courts that have invalidated state "harm to minors" laws governing Internet speech have expressed great concern about the fact that standards vary significantly among different communities.[8] The district court in Pataki cited numerous examples of meritorious works that would be placed at risk under a "harmful to minors" standard, including "[f]amous nude works by Botticelli, Manet, Matisse, Cezanne and others." It noted that some communities have acted to protect their youth from I Know Why the caged Bird Sings by Maya Angelou, Funhouse, by Dean Koontz, The Adventures of Huckleberry Finn by Mark Twain, and The Color Purple by Alice Walker. Pataki, 969 F. Supp. at 179-180. In Engler, the court expressed concern that a "harm to minors" standard would threaten the free flow of information to teenagers about premarital sex (including such topics as contraceptives and abstention) and sexually transmitted diseases. Engler, 55 F. Supp.2d at 749.

The nature of Internet communication brings these differing community standards into sharp focus. As the Supreme Court noted, "when the UCR/California Museum of Photography posts to its Web site nudes by Edward Weston and Robert Mapplethorpe to announce that its new exhibit will travel to Baltimore and New York City, those images are available not only in Los Angeles, Baltimore, and New York City, but also in Cincinnati, Mobile, or Beijing – wherever Internet users live. Similarly, the safer sex instructions that Critical Path posts to its Web site, written in street language so that the teenage receiver can understand them, are available not just in Philadelphia, but also in Provo and Prague." Reno, 521 U.S. at 854 (citation omitted). Given the standards of the many communities that will be reached, publishers on the Internet must anticipate what might be considered "harmful to minors" in each of them and to "zone" their speech accordingly. This is particularly problematic if speakers face any type of sanction if they fail to "properly" label or zone their expression. I would expect many to comply either by zoning speech according to their best guess as to the standard of the least tolerant community, or simply to restrict what information they make available.

8/ ACLU v. Johnson 194 F.3d 1149 (10th Cir. 1999); Cyberspace Communications, Inc. v. Engler 55 F. Supp.2d 737 (E.D. Mich. 1999); ALA v.

There are further complications as well. How much of a website must be zoned? Or, to frame the question in the context of constitutional law, what constitutes the work "as a whole?" Are parts of websites to be placed in a different "zone" from the home page? How would this work if zoning is to be accomplished through the creation of a new TLD? These and other questions suggest that real world "harm to minors" laws, that primarily require adult magazines to be placed behind "blinder racks," do not translate easily to cyberspace.

For those who suggest that cyberzoning is nothing more than an exercise in labeling, and therefore constitutionally benign, I suggest reading Interstate Circuit, Inc. v. City of Dallas 390 U.S. 676 (1968), decided by the Supreme Court the same day as Ginsberg v. New York There, the Court struck down on First Amendment grounds a local ordinance that required films to be classified as either "suitable," or "not suitable for young persons.[9] The ordinance did not preclude the showing of "not suitable" films – it merely

---

Pataki, 969 F. Supp. 160 (S.D.N.Y. 1997).

[9] The classifications were further defined by reasonably detailed criteria that required the classification board to consider films "as a whole," and to determine, among other things, whether "its harmful effects outweigh artistic or educational values such film[s] may have for young persons." 390 U.S. at 681-682.

required the distributor to get a special permit. The Court held that the local standard was unconstitutionally vague, in large part because it was being considered as a model for other communities, each of which might adopt their own variations. It reasoned that if film distributors are unable to determine what the standard means they "run[] the risk of being foreclosed, in practical effect, from a significant portion of the movie-going public. Rather than run that risk, [the distributor] might choose nothing but the innocuous, perhaps save for the so-called 'adult' picture." Id. at 684. The end result for the medium, according to the Court, is that "[t]he vast wasteland that some have described in reference to another medium might be a verdant paradise in comparison." Id.

The lesson to be drawn from this is that there is nothing simple about a "simple law" to zone speech in cyberspace.

III. OTHER POLICY AND PRACTICAL CONSIDERATIONS

There are other significant issues associated with any zoning proposal that would be implemented using the domain name system. I will touch on this only briefly in deference to other participants on this panel. My main concern, however, is that content-based "zoning" by domain name would compromise the function of the DNS. The DNS is a technical system for managing Internet addresses, and it is not well-suited to the task of implementing national policies. It has become involved to a certain extent in facilitating dispute resolutions involving intellectual property issues, but that is a far different matter from adopting a uniform system to restrict access to content. If there is any type of "mission creep" that involves domain name registries in assessing what type of content is appropriate for a given domain, the system would break down. The DNS is - at least ostensibly - a privately run system, and it is far from clear how any type of legislative mandate would work in this context.

It is also vital to keep in mind that any such zoning approach would be imposed on a global medium. The international nature of the DNS makes it particularly unsuited as a vehicle for national content control policies. The 243 ccTLD managers would be unlikely to agree to become instruments of U.S. policy, no matter how meritorious it may seem. And if they decline to participate, any plan for mandatory zoning will be ineffective. Moreover, any effort to use the DNS to further U.S. policies would undoubtedly add to existing tensions as the relationships among international participants are still being defined.

Conclusions

Because there is no current legislative proposal for cyberzoning, this testimony represents my preliminary views on the subject. However, I believe that proposals to "zone" Internet speech are far more complicated than they often are portrayed, and, if implemented, would almost certainly cause adverse unintended consequences.

April Major is an attorney with the Federal Trade Commission's Bureau of Consumer Protection, Division of Marketing Practices. In this capacity she works on issues primarily related to Internet fraud and deception.

Formerly, Ms. Major served as a Visiting Assistant Professor at Villanova University School of Law where she taught Computer Law, First Amendment and Regulation in Cyberspace, the Legislative and Administrative Process (Clinic), and Digital Law. At Villanova, Ms. Major also served as the Faculty Director of the Global Democracy Project (GDP), a program dedicated to advancing the development of civil societies and promoting the rule of law through Internet technology. GDP initiated projects in many regions of Central and Eastern Europe, Costa Rica, Rwanda, and most notably in Bosnia where the Project has successfully implemented an operational Internet infrastructure through grants from the U.S. State Department and other institutions.

Ms. Major received her Bachelor of Science degree cum laude in physics from Moravian College, where she was a member of the Sigma Pi Sigma, the National Physics Honor Society, and her law degree from Villanova University School of Law, where she received the Herman Mitchell Schwartz Award (awarded annually to the person in the graduating class who, in the opinions of the faculty, has contributed the most to the achievement of equality of opportunity and treatment for women). Following law school, Ms. Major was the Director of Technology and Director of Operations for the Center for Information Law and Policy ("CILP"), an organization dedicated to exploring issues at the intersection of law and technology. Additionally, she served a two-year position as a Teaching Fellow at the Law School.

Ms. Major's scholarly interests focus on law and technology. Her most recent publications include "*Norm Origin and Development in Cyberspace: Models of Cybernorm Evolution*," "*Copyright Law Tackles Yet Another Challenge: The Electronic Frontier of the World Wide Web*," and "*Internet Red Light Districts: A Domain Name Proposal For Regulatory Zoning of Obscen*

Testimony of April Major

before the

Commission on Online Child Protection (COPA)

regarding

The Creation of a New Top Level Domain for Adult Content

June 8, 2000

Chairman Telage and Members of the Commission:

Thank you very much for inviting me to discuss the creation of a new top-level domain for adult material. My name is April Major and for the past several years I have taught Internet-related courses at Villanova Law School including a course specifically on the subject of the First Amendment and regulation in cyberspace. I have also written an article regarding the creation of a new top-level domain for adult material in which I explore the First Amendment ramifications of creating "Internet red light districts." Before I proceed, I must point out that while I am currently an attorney with the Federal Trade Commission, the views I express today are my own and not the Commission's; I testify today in my personal capacity and not in my capacity as a Commission attorney.

When considering the creation of a new top-level domain for adult material, one necessarily must proceed through a legal and normative framework to determine the constitutional permissibility of such a scheme and the level in which it protects children. While doing this today I highlight the practical concerns and policy issues associated with this task.

Who are the Actors?

Initially one must consider who will establish the domain to determine whether the undertaking implicates the First Amendment. Industry alone may create the new ".adult" domain, government alone may formulate law and enforce compliance, or both government and industry may collaboratively work together. I will discuss each approach, but only the latter two scenarios implicate the First Amendment due to government involvement.

Past practice demonstrates that business and consumers favor independent efforts by industry and view these efforts as successful in many circumstances. However, a formidable collective action problem often presents itself when industry acts alone without inherent economic incentives. The normative reality is that without powerful incentives, acting for the greater common good may not be enough to induce people to act when weighed against the personal sacrifices one makes when acting collectively. PICS is a good example of an effort undertaken by the private sector alone that faces the ambitious task of convincing sites to rate themselves. Without the lure of monetary gain, content providers have little incentive to burden themselves. Many critics feel that without the force of government action behind such an initiative, convincing the critical mass necessary to make a difference is nearly impossible.

Alternatively, the government alone could legally require the creation of the domain and enforce adult sites to relocate content with the threat of costly civil fines and/or significant criminal penalties. If government unilaterally takes this action, Internet users and content providers would most likely react unenthusiastically, and perhaps even negatively, due to a common sense of mistrust that unfortunately taints legislative interference with business on the Internet. Consider the Communications Decency Act ("CDA") of 1996 where regrettably online business and user norms were neither understood nor considered by government. The lack of industry's involvement in Congress' first attempt to protect minors from indecent material on the Internet proved particularly detrimental to the success of the legislation.

Since the CDA, government and industry have accomplished many cooperative and complementary efforts in the area of Internet regulation. The Internet policy community recognizes that without the dual strength of industry's influence backed by government enforcement, individual indolence is far more likely in situations, such as the present, that are not market driven. Furthermore, in this situation, government and industry can together minimize the burden on content providers of moving to the new domain—an essential component of a smooth transition. Thus, the realization of a ".adult" domain initiative likely rests upon, among other things, the joint efforts of government and industry. If this is the case, we may confidently conclude that indeed this Commission must consider the First Amendment.

First Amendment Concerns

At this point, let us consider the constitutional issues that accompany a ".adult" domain effort. Recall for the sake of completeness that First Amendment precedent treats indecency and obscenity very differently; obscenity remains unprotected by the First Amendment, while indecency enjoys free speech protection. The remaining provisions of the severed Communications Decency Act already make the knowing transmission of obscene messages to any recipient under 18 a crime.[1] Thus, the ".adult" proposal targets material the Supreme Court deemed harmful to minors ("HtM") in Ginsberg v. New York[2]-- or in other words, indecency. The First Amendment protects indecent material for adults, but not for children because community standards and precedent determined its inappropriateness and harm to minors. The First Amendment permits regulation of indecent speech, but only if the government satisfies certain criteria. The appropriate criteria depend upon one's approach to the issue--a content-neutral zoning approach or a content-based perspective. I discuss each separately below.

Zoning Approach

A zoning approach or a "reasonable time, place and manner restriction" avoids First Amendment strict scrutiny because of content-neutrality. Reasonable time, place and manner restrictions are constitutionally permissible provided government justifies the restrictions without reference to the content of the regulated speech, government narrowly tailors the restriction to serve a significant governmental interest and the restriction leaves open ample alternative channels for communication.[3] For instance, in City of Renton v. Playtime Theaters[4], the Supreme Court held that the ordinance mandating that adult theaters not locate within 1000 feet of each other was an appropriate form of time, place and manner regulation. The Court acknowledged that city government aimed the ordinance at preventing the secondary effects of the presence of these theaters in close proximity of each other, such as crime, prostitution and decreased property value, and was not content-based. Thus the Court found the ordinance constitutional as long as it served a substantial state interest and did not unreasonably limit alternative avenues of communication.

---

[1] 47 U.S.C.A. s 223(a)(1)(B)(ii).

[2] 390 U. S. 629 (1968).

One could analogize the creation of a new top-level domain to a city zoning adult theaters and stores. However, a zoning rationale for the domain initiative would probably not survive First Amendment scrutiny. In order for government to create Internet red light districts, precedent requires that government concentrate the zoning effort on ridding the community of the secondary effects that result from sex shops and adult movie theaters such as increased crime, decreased property values and prostitution. Congress created the COPA Commission for the very purpose of protecting children and thus one could hardly contend that an initiative recommended by the COPA Commission targets the secondary effects of indecent material and not the content itself.

Furthermore, one is hard pressed to come up with secondary effects of adult material on the Internet. The Internet has no geographic proximity. While a web community could feasibly deteriorate if a member began posting pornographic content, in general the only way web pages are "near" one another are through links--and typically adult sites only link to each other. My article maintains that a feasible secondary effect might be the general deterioration of the commercial and educational value of the Internet or a broad deterrence of Internet growth, but as many authors, I have seen my theory disproved over the past several years. E-commerce firms thrive side-by-side with online pornography in the .com domain and I have yet to hear of any negative secondary effects. This lack of secondary effects combined with the recognition that the business and policy communities instinctively relate a ".adult" domain effort with protecting minors on the Internet, ensures little chance of success for a content-neutral zoning approach.

Finally, in Schad v. Borough of Mount Ephraim[5], the Supreme Court declared unconstitutional a local time, place and manner ordinance that banned all adult theaters from every commercial district in the city. While the Court recognized the necessity of local police power, the Court noted in this case that local governments must exercise their authority within Constitutional limits. An unsettling similarity exists between preventing all adult web site operators from publishing in the .com domain and preventing all adult theaters from every commercial district in a city. This analogy provides a sound argument for adult web site operators who are against moving their materials out of the .com domain.

---

[3] Ward v. Rock Against Racism, 491 U.S. 781, 798 (1989).

[4] 475 U.S. 41 (1989).

[5] 452 U.S. 61 (1981).

Content-Based Approach

Thus, if a zoning framework does not satisfy First Amendment scrutiny due to a lack of content-neutrality, one may squarely approach a domain initiative as content-based regulation and thus subject to strict judicial scrutiny. The Court applies its most rigorous level of scrutiny, known as strict scrutiny, when the government regulates based on the content of speech. Under strict scrutiny, the Court determines whether the government has a compelling interest and if so, whether the regulation at issue is the least restrictive means for satisfying that interest. The Supreme Court in Ginsberg clearly acknowledged that protecting children from harmful materials is a compelling interest.[6] Thus, opponents of a new ".adult" domain would focus their efforts on showing that a new domain is not the least restrictive method of protecting children from harmful content. Instead, they would likely argue that filtering alone is less restrictive than filtering with the aid of a ".adult" domain. Admittedly filtering alone is less restrictive, however those in favor of the domain may challenge the current effectiveness of filtering technology alone. Supporters might point out that the new domain is simply a tool for parents to enable effective filtering of content that is harmful to their children. Ultimately the court decides whether such an effort survives strict scrutiny, but while opponents have solid arguments against government intervention, my impression is that supporters may very well convince the Court that a new domain is the least restrictive means for protecting minors from harmful content.

Content

Next, we must determine the content that belongs in the new domain. At this point I emphasize the necessity of an international scheme in order for the effort to succeed and provide an effective tool for parents. The U.S. cannot create a system alone and expect any level of efficacy due to the well-known fact that much pornographic content on the Internet originates from overseas. However, the U.S.' participation in an international effort may not infringe upon constitutionally protected speech or undercut the First Amendment rights of its citizens. In other words, if an international agreement adopts a broader definition of HtM than provided in Ginsberg, the U.S. may not constitutionally adhere to the agreement because it would restrict protected speech. Thus, such an agreement may adopt the Ginsberg test or a less restrictive definition to evaluate content and remain constitutionally permissible.

---

[6] 390 U.S. 629, 646

Recall that the Ginsberg definition of HtM is the Miller obscenity test with "as to minors" tagged onto each prong.[7] Applying this test to the Internet is extraordinarily difficult, if not impossible because, among other things, it considers "community standards." While in real space it might make sense to allow communities autonomy in determining what they consider "appeals to the prurient interest," virtual space does not lend itself to evaluating geographic community norms. Thus, an international agreement would have the best chances of succeeding if it adopted a per se rule, as advocated by Bruce Taylor in the past, that allows for greater certainty and better notice to online content providers. [8]

Conclusion

Given the current inadequacies with filtering technology, I have no doubt that if the domain were in place, parents could more effectively control the content children view on the Internet. While I believe there are serious concerns involved in creating a ".adult" domain, I do not believe they are insurmountable. With careful planning, collaboration between the private and public sector, consideration of the norms of cyberspace, and coordination with foreign governments, I believe a ".adult" domain may succeed in protecting minors from harmful content while providing First Amendment protection of speech for adults.

---

[7] In Miller v. California the Supreme Court defined obscenity as (1) whether the average person, applying contemporary community standards, would find that the work taken as a whole, appeals to the prurient interest; and (2) whether the work depicts or describes in a patently offensive way, sexual conduct specifically defined by the applicable state law; (3) and whether the work taken as a whole lacks serious literary, artistic, political or scientific value. 413 U.S. 15 (1973).

[8] Grouping a good deal of content into one category is an impending issue that raises constitutional concerns. Certainly differences exist in what is harmful to a 6 year old and what is harmful to a 16 year old. My sense is to leave this to parents who many adjust the granularity, if you will, of their filtering software as their child grows older, perhaps allowing their child more access to ".adult" as the child grows older.

"NLC"

NATIONAL LAW CENTER
FOR CHILDREN AND FAMILIES
3819 Plaza Drive, Fairfax, VA 22030-2512
(703)691-4626, Fax: -4669
BruceTaylor@NationalLawCenter.org

BRUCE A. TAYLOR

Bruce Taylor is the President and Chief Counsel of the National Law Center for Children and Families.[1]

He was most recently a Senior Trial Attorney for the Child Exploitation and Obscenity Section of the U.S. Department of Justice.[2] Mr. Taylor first served as a Prosecutor and Assistant Director of Law for the City of Cleveland, prosecuting several hundred obscenity cases and appeals, including an argument before the United States Supreme Court.[3] For ten years, Mr. Taylor was then General Counsel to Citizens for Decency through Law, Inc., where he assisted prosecutors, police, and legislators nationwide in the enforcement, investigation, and improvement of laws against obscenity, child pornography and exploitation, and child sexual abuse.[4] He also served as Assistant Attorney General of Arizona. Since 1973, he has prosecuted nearly 100 state and federal obscenity jury cases, as well as trials on prostitution, RICO, child pornography, and child sexual abuse, has written over 200 appeal and *amicus curiae* briefs, presented over 50 appellate arguments, and has represented public officials and law enforcement personnel in civil lawsuits on civil rights, zoning, nuisance abatement, injunction and forfeiture actions, criminal procedure, and federal challenges to federal, state, and municipal laws.

---

[1] At NLC, he provides specialized prosecution and First Amendment advice and litigation assistance to federal, state, and local prosecutors, law enforcement officers, and legislators on obscenity, child pornography and sexual exploitation, as well as Internet and broadcast communications law issues. He has filed numerous *amicus* briefs in the U.S. Supreme Court, as well as federal and state appellate and trial courts across the Country. He has also been legal advisor to Senate and House sponsors of Internet, obscenity, and child exploitation bills and is *Counsel of Record* on BRIEFS FOR MEMBERS OF CONGRESS AS *AMICI CURIAE* in support of the Communications Decency Act (CDA) in *ACLU v. Reno* (E.D. Pa. 1996), *Shea v. Reno* (S.D.N.Y. 1996), and *Reno v. ACLU*, 521 U.S. 844 (1997), and for the Child Online Protection Act (COPA) in *ACLU v. Reno* (E.D. Pa. 1999) and (3d Cir. 1999).

[2] While at DOJ, he was co-counsel in the following trials: *U.S. v. Reuben Sturman, et al.* (D. Nev.), a federal obscenity-racketeering-conspiracy case against the world's largest hard-core porn distributor; *U.S. v. Larry Lane Bateman* (D. N.H.), a child pornography case against a Phillips Exeter Academy drama teacher, and *U.S. v. Frederick Yazzi* (D. Ariz.), a multi-year child abuse case in Indian Country.

[3] Before the Supreme Court, he argued *Larry Flynt v. Ohio*, 451 U.S. 619, in 1981. He successfully defended the Ohio obscenity statute before the Ohio Supreme Court in *State of Ohio v. Burgun* (1978) and before the U.S. Court of Appeals in *U.S. v. Sovereign News Co.* and *Turoso v. Cleveland Municipal Court* (6th Cir. 1982), *cert. denied* 1982.

[4] While at CDL, he was special prosecutor and co-counsel in dozens of jury trials in several states and presented oral arguments before the Ohio and Colorado Supreme Courts and the U.S. Courts of Appeals for the Sixth and Ninth Circuits, as well as presenting numerous law enforcement seminars, legislative testimonies, and media appearances.

The President's Pen

It was a nice, hot summer. A good time to fight pornography; a bad time to watch pornographers get richer and more airtime on television. They have an ogre's foothold on the "dot.com" domain of the World Wide Web. Now they want their own domain and many good people think it would be an acceptable compromise to have a red-light district zoned into the Web forever. Sounds like what Chamberlain gave to Hitler, the Sudetenland for peace. "That's all we want and we'll leave you alone." Give them a "dot.porn" and they'll be easy to spot and filter and block out and we can keep our kids and grandchildren out of that combat zone. I don't like the smell of it. When our 7 year old daughters and 4 year old grand-daughters are taught in Computer Tots class that there is a special place on the Internet where kids shouldn't go, they'll ask us what that means. How will we explain that there are "adult" pictures they shouldn't see on all the "dot.sex" sites? Do we ask -please don't look at any of those hot-links you're offered when searching for "toys" or "teen" or "girl" stuff? Will they be impressed that a "dot.xxx" domain was created by responsible adults in their parents' generation, that this special zone was set up by our lawmakers and is a wonder of technology figured out by brilliant computer geniuses in our universities and by the kingpins of the Internet industry? Will they believe us when we tell our little loved ones that this was all done "for the children" or do we confess that it was done to accommodate men and boys who like to look at dirty pictures of girls their age or the ages of their older sister or cousins? Do we say we were scared or tired or just gave up fighting to stop what the Supreme Court called the "crass commercial exploitation of sex"? Do we laugh it off as "boys will be boys" or make sarcastic remarks about the price we pay for freedom? Should we preach a "right" for "adult entertainment" to sell pictures of girls without their clothes on and that this is just another part of the Constitution that founded our great Country. America will cease to be great when it ceases to be good. True enough. We aren't done fighting yet. We filed four good and tough *amicus* briefs this summer. We were your "friends of the court" in cases fighting porn teasers on commercial Websites (*ACLU v. Reno*), fighting porn signal bleed that cable companies won't scramble (*US v. Playboy*), fighting immunity for Internet Service Providers who refuse to police their own networks yet want the courts to protect them under the "Good Samaritan" law (*Lunney v. Prodigy*), and fighting to restore the right of cities to prohibit strip-joints from hiring young women to gyrate naked in "gentlemen's clubs" and call it "nude dancing" (*City of Erie v. Pap's AM*). I think we should keep fighting the porn syndicates. I don't think we can trust pornographers to stay in their "zone" and I'm afraid most parents, schools, and libraries won't use filters on all the children's computers. I also can't forget that the good citizens and business owners who are stuck next to the infamous Combat Zone in Boston are still fighting to move that red-light district out of their neighborhood, after a quarter century of such "combat." We should bring back the "banned in Boston" obscenity and prostitution prosecutions and push the criminals back out of the free world. I don't want to give Hitler someone else's homeland and hope he makes no further demands. I don't want to hope he leaves us alone if we appease his lust for power and money. It doesn't work that way. We gotta fight them.

See you on the ramparts,
Bruce

BEST COPY AVAILABLE

BIOGRAPHY FOR DAVID G. POST

David Post is currently an Associate Professor of Law at Temple University Law School, where he teaches intellectual property law and the law of cyberspace, and a Senior Fellow at the National Center for Technology and Law at George Mason University. He is also the Co-Founder and Co-Director of the Cyberspace Law Institute <http://www.cli.org>,Co-Editor of ICANN Watch <http://www.icannwatch.org>, and Co-Founder and Co-Director of Disputes.org <http://www.disputes.org>.

Trained originally as a physical anthropologist, Professor Post spent two years studying the feeding ecology of yellow baboons in Kenya's Amboseli National Park, and he taught at the Columbia University Department of Anthropology from 1976 through 1981. He then attended Georgetown Law Center, from which he graduated *summa cum laude* in 1986. After clerking with then-Judge Ruth Bader Ginsburg on the DC Circuit Court of Appeals, he spent 6 years at the Washington D.C. law firm of Wilmer, Cutler & Pickering, practicing in the areas of intellectual property law and high technology commercial transactions. He then clerked again for Justice Ginsburg during her first term at the Supreme Court of the United States before joining the faculty of, first, the Georgetown University Law Center (1994 1997) and then the Temple University Law School (1997 – present).

Professor Post's articles on intellectual property, the law of cyberspace, and the application of complexity theory to Internet legal questions, have appeared in the Stanford Law Review, the Journal of Legal Studies, Esther Dyson=s *Release 1.0*, the Journal of Online Law, the University of Chicago Legal Forum, the Vanderbilt Law Review, the Georgetown Law Journal, and numerous other publications. For four years (1994 - 1998) he wrote a monthly column on law and technology (APlugging In@) for the *American Lawyer*. He has appeared as a commentator on the law of cyberspace on such programs as the Lehrer News Hour, Morning Edition, PBS= ALife on the Internet@ series, NPR's All Things Considered and MarketPlace, and Court TV=s Supreme Court Preview. During 1996-1997 he conducted, along with two colleagues (Professors Larry Lessig and Eugene Volokh) the first Internet-wide e-mail course on ACyberspace Law for Non-Lawyers@ <http://www.ssrn.com/update/lsn/cyberspace/csl_lessons.html> which attracted over 20,000 subscribers. He also plays guitar, piano, banjo, and harmonica in the band ABad Dog@ <http://www.mp3.com/BadDog1999/>.

Professor Post=s writings can be accessed online at <http://www.davidpost.com>.

Written Testimony
Submitted to the Commission on Child Online Protection

June 8, 2000

David G. Post

Thank you for the opportunity to address the Commission . I speak to you both as a parent of two minor children, and as someone interested in the continued expansion of the remarkable communicative potential of the Internet. Efforts by the Commission to assist us in understanding, and in making intelligent use of, the "technologies and methods that might be used to help reduce access by minors to online materials that are 'harmful to minors,'" to quote from the Commission's terms of reference, are of the deepest importance.

The situation, as I understand it, is as follows:

1. There is readily-accessible material on the Internet that we would all agree is "harmful to minors" (HTM).

2. There is readily-accessible material on the Internet that some reasonable people would claim is HTM -- or, perhaps, harmful to some minors but not others – while others would assert that it is not.

3. Congress seeks a *constitutional* way to eliminate, or at least to minimize, minors' access to HTM material (at least HTM material in the first category). Its first efforts – the Communications Decency Act and the Child Online Pornography Act – have been struck down by federal courts as unconstitutional infringements on the right to free speech.

4. Any solution must not interfere substantially, or more than is necessary to achieve the goal of limiting minors' access to HTM material, with communication by and among adults. Much HTM material is "constitutionally protected speech," and any State action that restricts adult access to such material is presumptively unconstitutional.

Any Congressionally-mandated action regarding this problem should have the following features:

1. It should recognize and respect differences of opinion as to what constitutes HTM material. These differences may be geographically-based: different local school boards, for example, will have, and should have, different views of the material that should be excluded from view by an eighth-grader. The differences may be non-geographical; followers of different religious traditions will continue to have different views as to what constitutes HTM material irrespective of geographic location, for example, as will individual parents on the basis of their own particular moral or ethical codes.

2. It should recognize that the primary responsibility for insuring that minors are not exposed to harmful material rests with parents, educators, and others in a care-giving role. In real-space, it is not the law that serves as the primary constraint on minors' access to harmful material, it is the combined effects of the culture created by parents, teachers, peers; the government's role is primarily to facilitate the reasonable exercise of that control. That should be the goal in cyberspace as well.

The Domain System and HTM material

1. The current configuration of the domain name system, in particular the existence of 7 top-level domains (TLDs) (.org, .com, .net, .mil, .gov, .int, .edu), is not technically mandated. There is no technical reason that there could not be hundreds, or thousands, of TLDs. ICANN is currently considering proposals to enlarge the number of TLDs.

2. Expansion in the number of TLDs is a desirable policy objective for many reasons having little or nothing to do with this Commission's inquiries. Expansion will, for instance, reduce the level of

conflict over the "rightful ownership" of particular second-level domains (*xyz.com*, *university.edu*, etc.), and it will allow a greater degree of self-differentiation of Internet services than is possible given the current artificially-maintained TLD scarcity.

3. Expansion in the number of TLDs would permit experimentation with a familiar technique for restricting minors' access to HTM material, a kind of Internet "zoning." In real-space we often use a strategy of requiring material that is appropriate only for adults to be spatially (as in 'red light' zones) or temporally (as on the federally-regulated radio broadcast spectrum) segregated.

4. If, somehow, we could arrange things such that all HTM material – however we would define that category -- were segregated into specified TLDs, it would then be a relatively trivial task to configure individual browsers so as to deny access to those TLDs, and hence to that material.[1] At the same time, the material would still be "there," available to those who wish to access it.

5. Would this solution – again, assuming for the moment that it is attainable – be constitutional if it resulted from direct congressional decree, e.g., a law requiring individuals distributing material that is "harmful to minors" to place that material within specified top-level domains? I am no constitutional scholar, and I would defer gratefully to others on that question; my reading of the cases, most importantly *Renton v. Playtime Theaters*, 475 US 41 (1986), suggests that such a law would pass constitutional muster. Precisely because zoning does not restrict adults (or children who have a supervising adult's permission) from "entering" the HTM zones, the burden on protected speech – the primary constitutional vice of COPA and the CDA – is minimized if not eliminated.

   (a) Even if such a law could achieve its objective of segregating all HTM material into specified domains, it would not, obviously, keep all minors from accessing HTM material. That it is a less-than-perfect solution to the problem should not, however, affect our view of its constitutionality.

If this were our goal, is it achievable? What steps might Congress take to help achieve it?

1. First, TLD-space must be enlarged. In the current configuration, Internet "real estate" (in the form of TLDs) is too valuable to "waste" an entire domain on HTM material. As noted above, expansion is currently on ICANN's agenda, and ICANN could, usefully, be encouraged to act rapidly on expansion plans.

2. Because that TLD expansion has not yet taken place, and because the manner in which it does take place (and, indeed, whether or not it does take place) is not entirely within Congress' control, it is difficult to specify precisely the steps that Congress could or should take to facilitate this zoning. Thus, for example, even if ICANN adopts an expansionist policy with regard to new TLDs, it is not clear whether new TLDs will be restricted, or unrestricted, in number; whether ICANN itself will designate the name(s) of the new TLDs or allow individuals to propose their own names; whether ICANN will accept proposals for new TLDs on a first-come, first-serve basis, or will utilize a lottery, or auction, or some other method for allocating responsibility for management of the new TLDs; whether ICANN will permit governmental institutions to operate new TLDs; etc. The answer to these, and many other, questions will at least partially determine the means that Congress can use to facilitate the segregation of HTM material into particular TLDs.

3. Assuming that additional TLDs become available, how can Congress encourage the segregation of HTM material into specified domains? And which domain(s)?

   (a) First, and most simply, Congress could authorize the maintenance of a public list of "designated HTM TLDs," a set of *pointers* to domains containing HTM material. The list of designated HTM TLDs could then serve as an authoritative source of information for parents (or anyone else) seeking to avoid HTM material. Browsers could relatively easily be re-configured, or built, to contain an automated "lock-down" option whereby access to a designated HTM TLD would be denied; if the browser market failed to produce such an option (as I suspect it would), browser manufacturers could be "encouraged" to provide the option in their products.

---

[1] At least as to material on the World Wide Web. Newsgroups, for example, do not rely on domain identification in the way that web servers do, and a domain-name-based solution to the problem of HTM material on newsgroups would have to take a very different form (if it could be achieved at all).

(b) My guess – and it is, and can probably only be, just a guess – is that a significant amount of HTM material would "migrate" to the designated HTM TLDs without any express legal requirement that it be placed there.

(c) Congress could, alternatively, expressly mandate placement of HTM material in the designated HTM TLDs. For example, a statute could simply require that all HTM material be placed into one or more TLDs specified in the statute, or appearing *ex post* on the list of designated HTM TLDs. Alternatively, as it did in COPA itself, Congress could define the offense of distributing HTM material and provide that placement of such material in one of the listed domains is an affirmative defense to criminal or civil liability under a re-enacted COPA.[2]

(d) My own preference would be to postpone implementation of an express legal requirement of this kind until we have more experience with the effectiveness (or lack of effectiveness) of a scheme involving voluntary, uncoerced segregation of HTM material into the designated domains. While this might appear to be a somewhat weak-kneed approach to the problem at hand, it could well do considerable good (while doing little harm). It is a means by which the government can provide the one thing that is in short supply on the Internet: tools for coordinating the action of large numbers of like-minded individuals. The mere existence of the set of pointers may serve as an effective catalyst for the accumulation of a substantial amount of HTM material in the designated domains. The extent to which this solves the problem of control over minors' access to this material can be assessed *ex post*, and more vigorous means employed if necessary.

4. The difficult question becomes: how is this list of designated HTM TLDs to be maintained? How do TLDs get on, or off, the list?

(a) Congress could delegate to a federal agency the task of searching and locating HTM material for the purpose of placing TLDs in which such material is found onto the list of designated HTM TLDs.[3] Even aside from the unseemliness of having government officials seeking out material of this kind, this approach has any number of associated problems. The operators of individual TLD registries have only a limited degree of control over the material that appears there; any individual TLD is likely therefore to have a diversity of information content, *i.e.*, some sites that do, and some that do not, contain HTM material. What threshold – 1% of material? 5% of material? 10%? – will be used to determine whether or not a TLD is given the HTM designation? How will that be measured? Many TLD registry operators are likely to resist classification as an HTM designated location (especially if the threshold is low enough), and to fight, through administrative or judicial procedures, any such classification. Whatever the chosen threshold, a significant amount of material is likely to be mis-classified under such a scheme.

(b) If the goal is to *punish* registries for allowing HTM material to appear in their domains this might be an appropriate way to proceed; but the goal is not to punish them for hosting constitutionally-protected material but rather to encourage the segregation of material into identified domains.

---

[2] In COPA itself, the offense -- "knowingly and with knowledge of the character of the material . . . mak[ing] any communication for commercial purposes that is available to any minor and that includes any material that is harmful to minors" – was made subject to an "affirmative defense": "good faith" steps taken to "restrict[] access by minors to material that is harmful to minors," including (a) requiring use of a credit card, (b) accepting a digital certificate verifying the user's age, or (c) "any other reasonable measures that are feasible under available technology." COPA, Sec. 231(c). Placement of material in a designated HTM TLD could be added as an additional affirmative defense to prosecution or to civil liability under a revised COPA.

[3] Appropriate notice and appeal procedures, it goes without saying, would have to be provided.

That can better be accomplished by instituting a procedure under which domain registries self-identify themselves through a simple application procedure, and placed on the list at their own *request. It is perhaps unfortunate, but nonetheless true,* that there will be commercially-operated domains that will welcome such an "official" designation as a way of signaling to potential consumers that hard-core material can be found at that location, and at least a substantial number of those with HTM material for sale will be willing to forego making their material available to minors for what they would see as the benefit of being easily locatable by their primary adult consumers.

(c) I do not see, in other words, any compelling reason, at least in the first instance, for the government to do more than to endorse the self-identification of individual domains as containing HTM material. I think it reasonably certain that a substantial amount of HTM material would make its way into those domains precisely because they can be found easily by consumers; that will enable those who wish to avoid this material to do so with relative ease.

(d) This is a small step, to be sure. But small steps are the most appropriate when walking on rapidly-changing and uncertain terrain. This will not create a world in which no minors encounter material on the Internet that may be harmful to them; but nothing Congress does can create such a world. It is minimally intrusive on the rights of adults to communicate in whatever ways they wish, and avoids entangling the government in making content-based determinations that are, at the very least, in some tension with the command of the First Amendment. It can help to bring a degree of order to the Internet in a way that many parents and educators will find useful; how much order, and how useful, cannot be predicted in advance. If it is entirely ineffective at achieving its goal, it can be abandoned, or supplemented with additional measures, in the future.

Testimony of
Mark MacCarthy
Senior Vice President for Public Policy

Visa U.S.A.

Before the
Commission on Online Protection

June 9, 2000

My name is Mark MacCarthy. I am Senior Vice President for Public Policy at Visa U.S.A. Thank you for the opportunity to testify before you today on the important topic of measures to verify age on the Internet.

I understand that the Commission was created by the Child Online Protection Act, which was approved by Congress in October 1998. The primary purpose of the Commission is to "identify technological or other methods that will help reduce access by minors to material that is harmful to minors on the Internet." The Commission's report on these matters is due to Congress by November 30, 2000.

Visa U.S.A. is supportive of the Commission's mission and is prepared to be as helpful as we can to further its work. It is in this spirit that I am testifying before you today.

Let me start by describing what I take to be the background for the use of payment cards as a mechanism for verifying age under the Child Online Protection Act. This Act is designed to prevent a person who is a minor from accessing materials that are "harmful to minors" over the Internet. Under the Act, a defendant can assert an affirmative defense to prosecution under the Act by showing that the defendant has made a good faith effort to restrict access by persons under the age of 17 to obscene materials on the defendant's Internet site. One way for the defendant to assert this affirmative defense is to show that the defendant required use of a credit card or a debit card to access the Internet site. In providing so, the Act basically assumes that only adults have access to a credit card or a debit card.

To the contrary, it is important for the Commission to understand that this assumption simply is not correct. Access to a credit card or a debit card is not a good proxy for age. The mere fact that a person uses a credit card or a debit card in connection with a transaction does not mean that this person is an adult.

Many individuals under the age of 17 have legitimate access to, and regular use of, credit cards and debit cards. For example, parents may designate their child as an "authorized user" of the parent's credit card or debit card. This actually is quite common, particularly for credit cards. Whenever this occurs, the child will have access to the parent's credit card number or debit card number and can use that card number to access materials deemed "harmful to minors" on the Internet.

In addition, many children under the age of 17 have their own deposit accounts and may have access to a debit card that accesses such account.

Moreover, using access to a credit card or debit card as a proxy for age actually could result in an inadvertent commission of criminal acts. Unauthorized use of a credit card is a criminal offense. If, for example, a child makes the mistake of using his or her parent's credit card without the parent's knowledge, and the parent later reports that unauthorized use, a criminal investigation might ensue before the true nature of the problem was discovered.

This not only would divert scarce enforcement resources from more important concerns, but also could create problems for the child and the family that are unrelated to and in addition to the harm against which the Act seeks to protect.

I am not here before you today to seek to revise legal situation regarding the use of payment cards as age-verifiers under the Act. The mandate of the Commission is broader than the Act, however, and requires the Commission to report accurately and completely regarding the effectiveness of various technologies in preventing access by minors to matter that is harmful to them.

Thus, although the Act assumes that only adults have access to a credit card or a debit card, it is important for the Commission to understand that this assumption is simply not true. As a result, the Commission may want to focus its attention on more suitable methods of verifying age.

Thank you for this opportunity to testify before you today on this important topic.

Michael Scott Baum
VeriSign, Inc.
1350 Charleston Road
Mountain View, CA 94043
Tel. 650-429-3444
Fax. 650-429-5113
Net. michael@verisign.com

Michael S. Baum serves as Vice President of Practices and External Affairs, VeriSign, Inc. His responsibilities include developing and overseeing practices and controls under which VeriSign conducts its Digital ID and VeriSign Trust Network operations; and legislative oversight.

Mr. Baum serves as *Chair*, Information Security Committee within the American Bar Association; a *Commissioner*, the Electronic Health Network Accreditation Commission; *Chairman*, International Chamber of Commerce (ICC) ETERMS Working Party, an *Observer Delegate* to the United Nations Commission on International Trade Law (UNCITRAL) on behalf of the ICC; *Member of the Board of Directors*, the PKI Forum, and a member of various digital signature legislative advisory committees.

Mr. Baum is *co-author* (with Warwick Ford) of Secure Electronic Commerce (Prentice Hall, 1997), *primary author* of VeriSign's Certification Practice Statement (1996), *author* of Federal Certification Authority Liability and Policy – Law and Policy of Certificate-Based Public Key and Digital Signatures (NIST, 1994), *co-author* of Electronic Contracting, Publishing and EDI Law (Wiley Law Publications, 1991), *contributing author* to EDI and the Law (Blenheim Online, 1989), and the *author* of diverse information security publications including the first American articles on EDI law. He served as *Guest Editor* for the Jurimetrics Journal *Symposium on PKI* (July 1998); honored as an *EDI Pioneer* in 1993 (EDI Forum), and recipient of the National Notary Association's *Achievement Award*. He is a member of the Massachusetts Bar, an MBA graduate of the Wharton School, and a Certified Information Systems Security Professional (CISSP).

Child Online Protection Act

TO: Commission on Online Child Protection

FROM: Michael S. Baum
Vice President, VeriSign, Inc.
michael@verisign.com

RE: Comments on Verification Systems

DATE: June 5, 2000

I. Introduction

This paper[1] responds to the Commission on Online Child Protection's (Commission) request for comments regarding "one-click away" resources, age verification systems, and an adult top-level domain in support of the Child Online Protection Act (COPA).[2] Specifically, it describes how digital signature technology might be used to support age verification systems under COPA.

This memo's main proposition is that only digital signatures[3] and supporting public key infrastructures (PKIs)[4] can provide adequate and scalable security for information communicated over open systems such as the Internet, and in particular, are well-suited to support COPA age verification requirements.[5] With few exceptions, only asymmetric cryptography (the technology upon which digital signatures are based) can provide strong support for nonrepudiation.[6]

---

[1] This paper is available at < http://www.repository/pubs/copa >.

[2] 47 USC § 231.

[3] Digital signatures utilize a key pair consisting of a key that is kept secret by its holder (the *private key*) and a corresponding key that is (or can be) made public (the *public key*) without compromising the private key. To digitally sign a message, the signer applies his or her private key to it. The digital signature is not the private key itself; rather, it is a number, unique to that particular signed message, that is generated when the private key is applied to the message. Therefore, every digitally signed message contains a unique digital signature. It is computationally infeasible to ascertain a user's private key by evaluating a digital signature from one of his or her messages. See Information Security Committee, Section of Science and Technology, American Bar Association, Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Secure Electronic Commerce § 1.11 (1996), < http://www.abanet.org/scitech/ec/isc/digital_signature.html >.

[4] The term *public key infrastructure* refers "both to a certification infrastructure based on public and private cryptographic keys and to the discrete components of such an infrastructure, including certification authorities, certificates, digital signatures, and the hardware and software that implements the infrastructure." *See* Michael S. Baum & Warwick Ford, *Public Key Infrastructure Interoperation*, 38 Jurimetrics J. 359, at 359 n.1 (1998), < http://www.verisign.com/respository/baum-ford6-28-99a.doc >

Digital certificates are highly flexible cryptographic tools, uniquely suitable for satisfying COPA's requirements. For example, digital certificates can be issued to:

> (1) *adults* to authenticate their having attained the age of majority (or any other mandated age), to permit their access to designated web sites and information resources and to exclude children, or
>
> (2) *children* (of any mandated age) to permit their access to designated web sites and information resources, to maintain parental control over children's access, and to exclude adults or other designated classes of persons from specified websites and resources.

In contrast, biometric technologies cannot by themselves secure open, distributed systems (such as the Internet), and PINs/passwords are inherently weak authentication mechanisms. Equally important, digital signatures can protect users' privacy, because (unlike biometrics) they can be communicated without disclosing personally identifiable information from the user.

In any technological system—and particularly one in which security is imperative—certain policy and deployment problems must be resolved if the system is to function properly. The deployment issues surrounding age verification systems for the World Wide Web are reconcilable within the current technological infrastructure of the Internet, if digital signatures and PKI are used as the tools by which age verification is achieved. Therefore we encourage the Commission to advance the use of digital signatures and PKIs as a preferable age verification mechanism for COPA purposes.

---

[5] The recipient of a digitally signed message may verify the authenticity of the message's digital signature (and thus of the message itself) by applying the signer's public key to the message and digital signature. Only the public key that corresponds to the private key used to sign the message will "match," thereby verifying the authenticity of the digital signature. To do this, the recipient must possess a copy of the signer's public key. One efficient way for a message recipient to obtain a copy of the signer's public key is by obtaining the signer's *digital certificate*. A digital certificate is simply a secured data record that contains the signer's public key, indicates the "binding" (or association) between that public key and the signer, and is itself digitally signed by the issuer of the certificate – a *certification authority* (CA).

[6] Nonrepudiation refers to substantial evidence of (1) the identity of the signer of a message and (2) message integrity, sufficient to prevent a party from successfully denying (i) having originated the message, (ii) that it was delivered, or (iii) the integrity of its contents.

II. Discussion

Public key technology is mature and commercially available

Public key–based technologies have been studied and used by the world's leading mathematicians and cryptographers in academia, industry, and government for many years.[7] For more than a decade, the Department of Defense has been using PKI-based applications to protect the nation's most guarded secrets. Public key–based security has also become ubiquitous in the commercial sector, and is now universally viewed as the predominant enabler of secure e-commerce and communications over the Internet. Governments, banks, universities, and many other users turn to digital certificates for secure e-mail, secure web access to databases, secure data submission via on-line forms, remote dial-up via secure virtual private networks, and many other applications.

To date, VeriSign has issued over 250,000 server certificates, used by web servers for secure and authenticated browser-based communications via SSL; the deployment rate for these certificates is now about 11,000 a month and is increasing by about 20% quarterly. As for individual "client" certificates (similar to those that could be issued to adults or children in satisfaction of COPA), VeriSign has issued nearly 5,000,000 to exchange secure mail, securely access web pages, submit data via secure forms, commute over the Internet to a corporate network, and many other applications.

Furthermore, the commercial PKI industry has established a track record of responding to accelerating demands for on-line security. For example, until recently, organizations wanting to deploy PKIs had to build, operate, and maintain their own PKI systems. The PKI industry responded to this need by making many high-quality security applications available on an outsourced basis, a much simpler and more cost-effective solution.

Two currently available, widespread PKI applications are particularly well suited to COPA's requirements:

---

[7] For example, the U.S. government has accepted PKI technology as the de facto standard for network security. The Deputy Secretary of Defense has released a policy mandate requiring all DOD users (over 2 million persons) to have a digital certificate by October 2001. Fielding is under way. Many agencies, including the Internal Revenue Service, the Securities and Exchange Commission, the Social Security Administration, and the Department of Veterans Affairs are moving forward with PKI projects. Additionally, the General Services Administration has awarded contracts to commercial certification authorities to issue certificates to citizens for secure on-line access to government benefits-related information and services. See < http://www.ec.fed.gov/aces.htm >. The Government Paperwork Elimination Act (GPEA) provides for federal agencies to give persons who maintain, submit, or disclose information the option of doing so electronically. GPEA requires the use of electronic signature methods, including digital signatures, to verify the identity of the sender and integrity of the associated electronic content.

- **Secure Web browsing** – Secure Web browsing using the secure sockets layer (SSL) protocol is already an integrated feature of nearly all commercial Web browsers. The SSL protocol relies on digital certificates to provide two-way authentication (the client knows the server to which it is connected, and the server knows the client to which it is connected) and confidentiality for all information communicated between the client and server. These security features are provided without additional effort by the client.
- **Secure e-mail** – Secure e-mail clients are interoperable using the leading secure messaging protocol (S/MIME). Like the SSL protocol, the S/MIME secure mail protocol is transparent to the users. By simply "clicking" on the desired "sign" and/or "encrypt" icons, the users can both digitally sign and encrypt their mail reliably and conveniently.

Validation of certificate holders

The efficacy of PKI rests largely on the reliability and practicality of the certificate validation process—that is, the process of approving or denying applications for digital certificates based on examination of certain specified credentials. The available validation options are quite broad and provide for great flexibility.

For COPA purposes, authenticating users' age is the key validation issue. The accuracy of the validations produced will depend both on the level of user effort required and on the overall creativity of the validation process. Ultimately there must be a determination of an appropriate level of accuracy to require, weighing the desired level of accuracy against the ease and costs of deployment.

Following are a number of methods for validating user age.[8] Many of these options can be merged to provide potentially stronger and more efficient results. There are theoretically an infinite variety of methods available to complete validation processes as a precondition to certificates deployment. Note that no matter which validation process is selected, it need only be performed *once*, then the validated information (e.g., age) is placed in the digital certificate in a non-forgeable manner such that it can be trusted to be accurate by *relying parties* in an infinite number of subsequent transactions.

- **Postal Clerks** – This approach is analogous to a postal clerk's current role in validating credentials for a passport. Certificate applicants would present proof of age to a postal clerk. The postal clerk would then examine the documents, query their holder, and either accept or reject the application. Post offices are in close proximity to most citizens, are generally perceived as trustworthy, and produce measurably uniform results.

---

[8] The order in which these are presented does not reflect any particular preference. Rather, these options are presented simply to demonstrate that significant flexibility exists in validation procedures.

- **Notaries Public** – Like postal clerks, notaries are ubiquitous and inexpensive. They provide comparatively strong assurances, since personal appearance of an applicant is required.
- **Other Trusted Persons** – Other trustworthy persons in a position to identify an individual would include that person's place of work, city clerks, school administrators,[9] and possibly bank trust officers.
- **Credit Agency or Government Databases** – In this approach, information that is generally unknown to the public is submitted by the applicant online, and the CA checks this information against credit agency or government databases to confirm the applicant's identity.

Biometrics

Biometric identification uses certain biological characteristics (like fingerprints or iris patterns) or behavioral traits (like signature dynamics) of individuals to verify their identity electronically. This technology is in an earlier phase of development than digital signatures and has particular complexities: "[i]n general, biometric identification requires sensors to convert a physical characteristic or behavior . . . into a signal that can be stored, or compared to previously stored signals, using a computer. Consequently, the detailed study of such devices requires the disciplines of human factors, biology, psychology, mathematics, statistics, and electrical and computer engineering."[10] The practical limitations of biometric technologies make them a poor choice to alone support the aims of COPA. Some biometric techniques do possess unique strengths that make them well suited to specific narrow applications, but by themselves they are insufficient to enable secure e-commerce – the strength and breadth of their security features are simply too limited.

---

[9] For example: After a parent or guardian applies for a digital certificate online on behalf of a child, the certification authority could send follow-up letters to the child's school (as designated in the application) and directly to the parent's home. The letters would contain different PINs. The letter sent to the school would be delivered home by the child, to confirm that the applicant is a parent. (That is, only someone with a child in school would receive such a letter.) The letter sent directly to the parent's home would verify that the applicant is who he or she claims to be. The parent would then enter the two PINs from the two letters into an enrollment form on the CA's web site to obtain the certificate. There are a number of possible variations on this theme that can produce useful results. See < www.cybersmart.org >.

[10] National Biometric Test Center < http://130.65.150.51/faculty/main/nbtc.html >. Dr. Jim Wayman notes that "DNA and all other 'forensic' identification techniques, including latent fingerprint identification, require extensive expert human processing and are not automatic. Therefore, they are not 'biometric identification techniques' according to the definition I use." E-mail from Jim Wayman, director, National Biometric Test Center, to Michael Baum (Nov. 29, 1998) (on file with author).

Moreover, biometric techniques do not themselves solve all the requirements for COPA. Biometric techniques do not lend themselves to readily include validated information (e.g., age) in the biometric signature without using cryptographic mechanisms, like digital signature, to bind them together. Also, biometrics themselves do not provide data integrity and encryption.

PKI offers distinct advantages over biometrics for diverse e-commerce applications, particularly global commerce conducted over the Internet. PKI offers a tested, extensible infrastructure that facilitates commerce conducted over unsecured paths. Therefore biometric technologies are unlikely to achieve the ubiquity of PKI, making them not only impractical but also inconvenient for the purposes demanded by COPA.

The PKI industry and most recognized cryptographers and security experts understand this and have long emphatically embraced the use of biometrics to *supplement and enhance* PKI security, rather than to substitute for it. Thus, biometrics are valuable for controlling local access to computer resources and cryptographic keys contained within a cryptomodule[11]; authorized users can then safely enable digitally signed or encrypted communications over insecure networks or channels, such as the Internet.

Privacy Considerations

It is essential that the technology used to support COPA not compromise an individual's privacy in any way. One cannot extinguish a fire by throwing kerosene on it! Any proposed solution must be closely scrutinized regarding its direct and indirect impact on the individual's privacy. Unlike some other technologies, digital signatures *do not necessarily require users to disclose personally identifiable information when accessing a Web site or other information resource*. They can serve as *age tokens* rather than *identity tokens*. The contrast between digital signatures and biometrics in the area of privacy is particularly stark, since biometrics requires the capture, communication and use of personal data. [12]

---

[11] *See* NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES (1994), *available at* < http://www.itl.nist.gov/div897/pubs/fip140-1.htm >.

[12] Also, "[b]iometric authentication technologies have limitations when employed in network contexts because the compromise of the digital version of someone's biometric data could allow an attacker to impersonate a legitimate user over the network." FRED B. SCHNEIDER, ED., COMMITTEE ON INFORMATION SYSTEMS TRUSTWORTHINESS, COMPUTER SCIENCE AND TELECOMMUNICATIONS BOARD, COMMISSION ON PHYSICAL SCIENCES, MATHEMATICS, AND APPLICATIONS, NATIONAL RESEARCH COUNCIL, TRUST IN CYBERSPACE, at ch. 7 (1998), < http://cryptome.org/tic.htm >.

Industry Self-regulation

With the recent acceleration and adoption of PKIs in both the public and private sectors, and perhaps with some modest encouragement from the Commission, the adoption of PKIs by Web sites and other information resource entities to assure the protection of children is promising. As the Commission becomes more familiar with the demonstrated capabilities of PKI, it can fashion proposed solutions that are less-burdensome and onerous to both the protected classes under COPA as well as to the industries that can enable such solutions. Consequently, it is urged that any proposed regulation be incremental and sensitive to the positive impact of commercial PKIs on available solutions. VeriSign is pleased to work with the Commission to further elaborate an appropriate solution that exploits the benefits of PKI.

About VeriSign

Information about VeriSign, digital signatures, and public key infrastructures is available at < http://www.verisign.com >.

***

Commission on Online Child Protection

6/22/00

Click here to start

Table of Contents

Commission on Online Child Protection

Agenda

Some Internet Security Threats

Digital Signature Technology

Digital Certificate

The Value of Public Roots

Terminology

Age Validation Options

Certificates: Advantages for COPA Purposes

Privacy Considerations

Biometrics

Information Security Committee American Bar Association

Summary

References

Author: Michael Baum

Home Page: http://www.verisign.com

Statement by
Pat McGregor
Chief Information Security Architect
Intel Corporation
Before the Commission on Online Child Protection
9 June 2000
Washington, D.C.

Mr. Chairman and members of the Commission, thank you for the opportunity to speak today before this hearing of the Commission on Online Child Protection. I am glad of the opportunity to offer you my insights into technologies for age verification and the processes that will be required to support them.

Introduction

The problem of age verification on the Internet is, intrinsically, no different from the problem authorizing any user based on a role or criterion they possess. Age verification is a special case only because of the sensitive issue of children's access to material that their parents or guardians might find objectionable. Otherwise, the processes and decisions which support accepting and validating credentials and granting appropriate access are the same faced by corporations, ISPs, and movie theatres. My 11-year-old son summarized the issue neatly the other day, when I asked him how he thought we could prove someone's age over the net. He said, "If we can't see them, how can we prove they aren't lying about how old they are?"

Authentication Methods

There are four major methods that could be reasonably used for identifying and authorizing access to material across the net. Those methods are, generally, ID and Password, Biometric, Digital Certificates, and Proxies. Let me discuss briefly each of these methods and their advantages and drawbacks.

ID & Password

IDs and passwords are acceptable for access to material that does not need to be protected with high assurance. They are, as most of us are aware, vulnerable to cracking, theft, and other attacks. In addition, humans don't use passwords effectively because of differences in ability to remember passwords, remember IDs, and the general unwillingness to use well-known security processes (such as frequent changes or one-time passwords) that make IDs and passwords more effective. On Internet scale, the logistical issues presented by 25 million children[1], each with an account on every site they might want to access, are too many to discuss in any depth. Even the prospect of a central credential storage and authentication service, similar to the Microsoft Passport, is subject to the problems with children remembering IDs and passwords and taking proper precautions to protect those credentials.

Biometrics

Biometric technologies offer some interesting advantages for identification and the creation of credentials that can be linked with a high degree of assurance to a given human being. However, even with adults whose facial characteristics are relatively stable from day to day, the problems of changing biometric characteristics from morning to evening make for problems with consistent authorization to assets. With children who can grow and change substantially from one month to the next, the problems of capturing and distributing valid biometric signature files for a rapidly changing population seem too complex for implementation on a large scale.

---

[1] Grunwald Associates. *Children, Families, and the Internet 2000 survey.* June 2000. http://www.grunwald.com/survey/survey_content.html

Digital Certificate

Digital certificates have the advantage over biometrics in that they are not based on characteristics that can change rapidly. They can be issued in a cryptographically secure fashion so that they are less vulnerable to cracking than other forms of credentials. However, certificates in isolation, separate from a security or authorization process, offer little advantage over any of the other forms of authorization and credentialing.

Proxies

I include proxies in this list because they can be configured to prevent access from a specific client to a given range of hosts. Parents find the use of proxies, or screening software, of value in preventing access to material they find objectionable when their children are surfing the Internet from home or school. The problem, of course, is when access is attempted from a client not behind the proxy, or when the password for the proxy is compromised and the filtering settings are changed.

Management Issues

The management issues and security processes for all of the authentication methods are the big obstacles in making any system of age validation work. Even in a corporation the size of Intel, with 80,000+ employees to track, we find that keeping credentials and access control lists current takes a major expenditure of staff resources. Multiplying the problem to include every child under 13 in the United States as well as every web server that might host objectionable material seems far too vast to be appropriately managed. Let me discuss some of the larger issues.

Security Process

Credentials can only be used to make a security decision in context of an appropriate security process. For example, look at the process you go through when you check a driver's license for identification. When you check a person's driver's license, you're doing a biometric test (face vs. picture). That involves: taking a sample (of the face), reading in the template (picture), and doing a comparison. You do all three of those steps inside your own body -- presumably an environment you have some assurance has not been compromised. When we do this sort of credential checking over the net, we must rely on some other entity -- a card reader, a biometric device, or a keyboard -- which is not under our control. The computer that the user wants to access must rely on another entity to take the sample or take in the credentials. It can compare the presented credentials against the records in its access database, but the process is as weak as the element that takes the sample -- and in the case of a computer in someone's house or school or library, that element is weak and untrustworthy.

Another security process we must look at is the issuing of credentials. If we mandate that children's credentials will be issued at, say, their school, we are requiring a security process infrastructure which most schools are not prepared to administer. Difficulties include the logistics of keeping track of highly transient populations, the varying implementation of the process in different school districts, and the fact that most school districts are barely funded for one computer technician, much less an administrator who will manage the issuing and revocation of credentials. In addition, not all children attend public school, and provision would have to be made for credentials for children at private schools, children who are homeless, undocumented aliens, or who do not attend school for other reasons, or who are home-schooled.

In addition to the simple mechanics of issuing and revoking credentials, we must consider that there may be disagreement over what age it is appropriate to begin issuing credentials. A Grunwald Associates survey this week says that children online range between two and seventeen years of age.[2]

---

[2] Martin Stone. More Online Kids, More Online Moms. E-Commerce Times, June 8, 2000. http://www.ecommercetimes.com/news/articles2000/000608-nb1.shtml

Do we issue credentials at birth? At entry into Kindergarten? When their parents purchase a home computer? How do we reconcile differing jurisdictions with differing standards or mandates?

Lost credentials

Human beings lose things. Children, in particular, lose things frequently. To be useful for allowing children access to the Internet in a protected fashion *wherever the child is* – not just at home or in the school – their credentials must be stored on some transportable media, such as a smart card, a watch fob (*a la* the fast sale gas pumps), or other easily carried item. If you have children, you can probably count the number of times they have lost sweaters, lunch boxes, house keys, and library books. I don 't want to think about how quickly my son could lose a plastic smart card, or how many times we would have to replace it in the course of a year.

Stolen or Forged Credentials

As my son said, one of the problems in this whole system is the fact that some people are not honest. They will lie about their age, their permissions, and their intent in accessing some material. We do not now have a good security process for identifying stolen or forged credentials (think of the bouncer at a bar reading driver's licenses, or a catalogue clerk accepting a stolen credit card over the phone, or the use of stolen telephone calling cards). If we go to a system where all children have children's credentials – or one where all adults have adult credentials – we must also implement a security infrastructure to do real-time validation of the credentials themselves, necessitating a reporting system where stolen credentials can be reported, forged credentials listed for confiscation, and new ones re-issued quickly.

Revocation of Credentials

When a child reaches 13 (or 18, under some proposals), they would no longer need credentials to validate their age. Some entity must revoke their credentials, in effect declaring them to be "old enough" to access any information they please. The logistical problem for this revocation can be highly complex. Can the school the child is in when they reach an acceptable age revoke the certificate, or must the school or post office or other agency make the revocation? Will all credentials be of the same manufacture, allowing for easy interoperability of systems, so that the revoking body can notify the issuing body that the certificate has been revoked? Or will the certificates expire on the date of the child's birthday, since the birth date must be known to issue an appropriate certificate? What happens if a school board in Oregon decides that the issuing school must actively revoke a certificate, while a school board in Florida uses an auto-expiration scheme? What will happen to the child who changes school districts? And what happens if the parents wish, for example, to keep controls on access for a child who is 13 but whom they feel is not sufficiently mature to handle adult material?

Global Issues

Since the Internet is a global entity, we must touch on the issues involved in giving access to materials outside the United States. It is in this global context that I fear most of the proposals to limit children's access to adult material will break down.

What is acceptable material for 13- or 18-year-olds in a European or Asian country may not be considered appropriate by parents (or school boards, or county boards of commissioners) in the United States. In fact, what is considered appropriate by many parents in Idaho may not match expectations of parents in Florida. We cannot enforce child protection guidelines in countries outside the US; therefore, there will always be a way for children to find adult material. Nor can we reasonably expect to limit or filter content based on domain name; we seldom use the ".us" domain identifier in the US, and many web sites based in other countries do not use their country's domain identifier. My expectation is that if the US tries to regulate access to content on US sites, the adult material sites will simply change their service providers to those based outside the US.

The nature of the Internet is that information can almost always be reached by taking a different path to the source. I am reminded of the policy of my local grocery store to hide the covers of Cosmopolitan, Fitness, and other magazines that sometimes have "suggestive" pictures on the front by using a metal face shield over the magazine rack. Interested children will go to a store without the blinder policy, or a library that carries the magazine, or to the home of a friend whose parents subscribe. Or, even, to the website for that magazine.

Roles and guidance

We cannot conclude any discussion of age verification and access by children to adult material without at least a brief discussion of the roles of various entities in the access decision process.

Familial values

It is at home where the real responsibility lies for age-appropriate access to the Internet and its resources. The adult responsible for a child should pay attention to their children's surfing habits, discuss what is and is not appropriate according to their family's value systems, and use the family discipline process to enforce that access. With all the problems cited above, the government (ours or any other) cannot take the place of this critical familial responsibility. It may be possible to provide a mechanism to assist in enforcing these family standards, but we have seen over and over again that "one size fits all" government standards are unworkable with the wide variety of family choices in the United States.

Schools

While it might be possible for schools, libraries, post offices, and other governmental entities to take on the role of credential issuer and manager, I am particularly concerned that schools, asked to take on yet another non-educational role, will simply be unable to resource the infrastructure required appropriately. We cannot ask teachers to add any more tasks into their days; they already have far too few minutes per day to actually teach. Public schools are marginally resourced for many of their functions today; a major influx of funding and staff would be required to handle this new responsibility.

Summary

There are many technologies for authentication and authorization on the market today, and more are being devised every year. The problem of age verification for children will require not only legislated standards for credentials, but also the implementation of an infrastructure that will support the use and management of these credentials. Before any steps to require age validation are taken by this commission, I strongly recommend that the implications and support requirements be evaluated in depth. Without the supporting infrastructure, any system to enforce age-appropriate access to online material will be unworkable, unenforceable, and an expenditure of resources that could more effectively be used elsewhere.

I leave you with one more thought from my personal management and child-raising philosophy. "Never give an order you can't enforce."

Thank you.

John D. Woodward, Jr., Esq.
RAND
703-413-1100 Ext. 5242 | Fax: 703-413-8111
woodward@rand.org
1200 South Hayes Street, Arlington, VA 22202-5050

John D. Woodward, Jr. is a Senior Policy Analyst at RAND, a non-profit institution that helps improve policy and decisionmaking through research and analysis. Mr. Woodward, an attorney, lectures and writes regularly on the law and policy concerns of biometrics. He is a co-author of RAND's study on U.S. Army biometric applications. In May 1998, he testified before a congressional hearing on "Biometrics and the Future of Money."

Mr. Woodward previously served as an Operations Officer for the Central Intelligence Agency for twelve years. His overseas assignments included tours in East Asia and East Africa. He speaks Japanese and Thai.

Mr. Woodward received his Juris Doctor degree magna cum laude from Georgetown University Law Center in Washington, D.C. He was a Thouron Scholar at the London School of Economics, University of London, where he received his M.S. in Economics. He has a B.S. in Economics from The Wharton School of the University of Pennsylvania. He served as a law clerk to the Hon. Roderick R. McKelvie, a U.S. District Court Judge in Wilmington, Delaware.

Mr. Chairman and Commission Members, thank you for inviting me to testify before this hearing of the Commission on Online Child Protection. I am honored to appear before you to offer my insights into biometrics.[1]

This Commission understandably wants to protect children from accessing online sites that are harmful to minors. As part of its effort, the Commission has correctly asked whether there are any kinds of commercially-viable age verification biometrics. The good news is there are many kinds of commercially-viable biometrics. The bad news is there are no age verification biometrics, no age determination biometrics and no age estimation biometrics.

As preparation for this testimony, I spoke with Dr. James L. Wayman, the Director of the National Biometric Test Center at San Jose State University. According to Dr. Wayman, no currently employed biometric technologies have any capability for age estimation. Wayman concluded, "It seems highly unlikely that the biometric identification technologies being employed today will ever have a capability for accurate age determination." In fact, one of the key attributes of biometric identification systems is that very little or no personal information is available in the submitted biometric sample.[2]

---

[1] John D. Woodward, Jr. is a Senior Policy Analyst at RAND. RAND is a nonprofit institution that helps improve policy and decisionmaking through research and analysis. This testimony is based on a variety of sources, including research conducted at RAND. However, the opinions and conclusions expressed are those of the author and should not be interpreted as representing those of RAND or any of the agencies or others sponsoring its research.

I recently discussed this same issue with Samir Nanavati, a leading biometric consultant. Mr. Nanavati stated that there are "no biometric systems that are capable of accurately determining a subject's age or age category (*e.g.*, under 18 years)." It is true that certain age groups and occupational groups have a more difficult time participating in some biometric systems. For example, a biometric system might have difficulty capturing or getting a fingerprint biometric from an elderly bricklayer. However, it does not appear that any commercially available biometric system or any system currently in development is able to use this degradation in performance to determine a person's age.

Special Agent Edward German of the U.S. Army's Criminal Investigation Division is one of our nation's leading fingerprint experts. When I interviewed him as preparation for this testimony, Mr. German stated that to his knowledge, "there is no reliable age determination set of factors based on the human body. Currently, there is nothing even close to reliable insofar as age and biometrics. There is not even something that gives a good indication."

---

[2] "Biometric identification" refers to the use of physiological characteristics and behavioral traits for the automatic identification or verification of individuals. In general, biometric identification requires

Even estimating age in a face-to-face context can be difficult. Common sense can help a cashier tell whether a person trying to buy alcohol is over age 21. But for many individuals in the age range of 16 to 21 years, personal habits, genetics, and environmental factors combine to preclude reliable age determination from physical attributes. In other words, nothing magically happens physiologically on a person's twenty-first birthday.

While the search for age determination and age estimation "metrics" is not an Internet-only phenomenon,[3] the Internet-driven need is for a reliable, remote verification of claimed age for a person likely to be unknown to the checker. As Peter T. Higgins, the former head of the FBI's Integrated Automated Fingerprint Identification System (IAFIS), has observed, "There might be some who advocate using a driver's license and comparing the person's face to the license photograph

---

sensors to convert a physical characteristic or behavior of a person into a signal that can be stored, or compared to previously stored signals, using a computer.

[3] To consider just one example, for many years, law enforcement has grappled with the problem of trying to determine the age of minors appearing in pornographic materials. To make this age determination, investigators used a list of features, such as facial and pubic hair, breast development, curvature of the hips, *etc.* Called "Tanner staging," after Dr. James Tanner who compiled the list, this physical feature screening for age determination has recently been abandoned at Dr. Tanner's urging because Tanner scaling is not designed for estimating chronologic age and, therefore, not properly used for this purpose. *See, e.g., Regional Task Force on Internet Crimes Against Children for Northern New England* available at http://www.ci.keene.nh.us/police/tannerscale.html (Tanner staging was designed for estimating development or physiologic age for medical, educational, and sports purposes, in other words, identifying early and late maturers. Tanner staging is appropriate for this, provided chronologic age is known.).

remotely through a camera and facial recognition software. The security concern, however, is that anyone can generate or purchase a false ID with a photo."[4]

It is possible that the time will come when secured databases will combine both a person's registered biometric and a verified age determination procedure to achieve the desired protective result.[5] For example, this age determination procedure could be done during enrollment when the person would physically appear at a center to enroll. But this approach does not depend on an age verification biometric but rather requires a vetted database in which known age data is used in conjunction with a biometric.

Although there is currently no reliable age determination biometric, there is one area of current scientific research that I want to call to the Commission's attention. This research involves the chemical compositions of fingerprints and highlights differences in physical characteristics between children and adults.

In layperson's terms, when a finger touches a surface, it may leave a latent fingerprint which is an invisible pattern of "oil," containing chemical secretions from the skin. These secretions can contain hundreds of chemical compounds. Researchers, led by Dr. Michelle V. Buchanan of the Oak Ridge National Laboratory, have concluded that there are dramatic differences in the chemical compositions of fingerprints from children and adults.[6] Dr. Buchanan believes that the dramatic differences between children and adult fingerprints can be explained by changes brought on by puberty. She believes she can determine when children are going through puberty by examining the chemical compounds in their fingerprints.[7] Research in this area continues.[8]

---

[4] *See, e.g.*, Susan Schmidt, "Probe Finds Security Lapses at Airport, Pentagon, FBI," *Washington Post*, May 25, 2000, at A2 ("Startling security weaknesses were discovered at two airports and all 19 of the federal agencies visited by special GAO investigators, who used counterfeit identification and phony law enforcement badges they obtained on the Internet.").

[5] For example, federal law requires that firearm background checks generally are to be conducted using a computerized system, known as the National Instant Criminal Background Check System

In conclusion, while an age verification biometric would seem to be the ideal "silver bullet" to protect children from accessing harmful online sites, there currently is no viable age verification biometric. While I am reluctant to underestimate the speed of technological advance, the experts seem to agree that an age verification biometric is at best a very long way from reality.

(NICS). *See* General Accounting Office, *Gun Control: Options For Improving the National Instant Criminal Background Check System*, GGD-00-56, Apr. 12, 2000.

[6] Adult fingerprints contain oilier, longer-lasting compounds, such as fatty acid esters, than children's fingerprints. Children's fingerprints contain more cholesterol and volatile chemicals, such as free fatty acids, than adults' fingerprints. Many of the chemical components released by children's fingers quickly evaporate, making it extremely difficult for law enforcement investigating crimes such as child abduction. *See* "Chemicals in Fingerprints Could Help Solve Crimes," *Science News*, Apr. 22, 2000; Michelle V. Buchanan, Keiji Asano, & Arthur Bohanon, "Chemical Characterization of Fingerprints from Adults and Children," *SPIE Photonics East Conference Proceedings*, Conference 2941, Nov. 1996, at 89-95. *See also* Deborah Noble, "The Disappearing Fingerprints," *Chem Matters*, Feb. 1997, at 9; Deborah Noble, "Vanished into Thin Air: the Search for Children's Fingerprints," *Analytical Chemistry*, July 1, 1995, at 435A.

[7] Analysis of the chemical composition of fingerprints might also provide (1) medical information (*e.g.*, explaining why some people's skin heals more quickly than others) and (2) a noninvasive way to test for certain medical disorders or presence of drugs (*e.g.*, nicotine). The research conducted to date has taught law enforcement investigators to look for children's fingerprints as soon as possible because they can quickly evaporate from a crime scene.

[8] Dr. Buchanan and her colleagues are continuing their research efforts. Recently, the Forensic Services Division of the United States Secret Service has also begun researching this area. Dr. Buchanan's research was supported by the Department of Energy's Chemical and Biological Nonproliferation Program (DOE NN-20).

I am happy to answer any questions you may have.

Jeffrey Dunn
Co-Chair Biometric Consortium

Jeff Dunn is Chief of the Identification and Authentication Research Branch at the National Security Agency. This group is researching new technologies to protect access to computer systems in the Department of Defense and other critical systems. During his 20-year career at NSA, he has held a variety of program manager and management positions. He is a graduate of the Agency's Management Development Program and certified as an Acquisition Professional. Mr. Dunn has provided consultations on biometric technologies to a wide range of Government organizations.

Statement by
Jeffrey S. Dunn
Fernando L. Podio
Co-Chairs, Biometric Consortium
Before the
Commission on Online Child Protection
9 June 2000
Washington, D.C.

Mr. Chairman and members of the Commission, we would like to thank you for the opportunity to speak today about biometric authentication technology. We believe this Commission's interest in biometric technology is very timely. Biometric technology is one means to achieve fast, user-friendly authentication with a high level of accuracy. Recent advances in biometric technology have resulted in increased accuracy at reduced costs.

Today, to address the Commission's interest in biometrics, we would like to discuss some of the terminology used by the biometric community, highlight some of the benefits of using biometrics for authentication, and give some examples of emerging applications and standards. We would also like to explain how the Biometric Consortium[1] is bringing together technologists from government and industry.

Introduction

Biometrics are automated methods of recognizing a person based on physiological or behavioral characteristics. Examples of human traits used for biometric recognition include fingerprints, speech, face, retina, iris, handwritten signature, hand geometry, and wrist veins. During **Enrollment**, a sample of the biometric trait is taken, processed by a computer, and stored for later comparison. Biometric recognition can be used in **Identification** mode, where the biometric system identifies a person from the entire enrolled population by searching a database for a match. For example, an entire database can be searched to verify a person has not applied for entitlement benefits under two different names. This is sometimes called "one-to-many" matching. A system can also be used in **Verification** mode, where the biometric system authenticates a person's claimed identity from their previously enrolled pattern. This is also called "one-to-one" matching. In most computer access or network access environments, verification mode would be used. A user enters an account or user name as usual, but instead of entering a password, a simple touch with a finger or a glance at a camera would be enough to authenticate the user.

Biometric technologies are positioning themselves as the foundation for many highly secure identification and personal verification solutions. Areas that will benefit from biometric technologies include network security infrastructures, government IDs, secure electronic banking, investing and financial transactions, wireless communications, retail, and health and social services. Highly secure and trustworthy electronic commerce, for example, will be essential to the healthy growth of the global economy. Many biometric technology providers are already delivering biometric authentication for a variety of web-based and client/server based applications to meet these and other needs.

Advantages of Biometrics for Authentication

Using biometrics for identifying human beings offers some unique advantages. Only biometrics can identify you as you. Tokens, such as smart cards, magnetic stripe cards, photo ID cards, physical keys, and so forth, can be lost, stolen, duplicated, or left at home. Passwords can be forgotten, shared, or observed. Moreover, today's fast-paced electronic world means people are asked to remember dozens and dozens of passwords and personal identification numbers (PINs) for computer accounts, bank ATMs, e-mail accounts, wireless phones, web sites, and so forth. Biometrics hold the promise of fast, easy-to-use, accurate, reliable, and less expensive authentication for a variety of applications.

There is no one "perfect" biometric that fits all needs. All biometric systems have their own advantages and disadvantages. There are, however, some common characteristics needed to make a biometric system usable. First, the biometric must be based upon a distinguishable trait. For example, for nearly a century, law enforcement has used fingerprints to identify people. There is a great deal of scientific data supporting the idea that "no two fingerprints are alike." Technologies such as hand geometry have been used for many years and technologies such as face or iris recognition have come into widespread use. Some newer biometric methods may be just as accurate, but may require more research to establish their uniqueness.

Another key aspect is how "user-friendly" a system is. The process should be quick and easy, such as having a picture taken by a video camera, speaking into a microphone, or touching a fingerprint scanner. Low cost is important, but most implementers understand that it is not only the initial cost of the sensor or the matching software that is involved. Often, the life-cycle support cost of providing system administration and an enrollment operator can overtake the initial cost of the biometric hardware.

Biometric authentication for age verification

With the current state-of-the-art in biometric technologies, there are no means to determine the age of an individual based on a physical or behavioral characteristic. Given the wide variability of human characteristics, it seems unlikely any that such technologies will be available in the future.

The most likely benefit biometric technologies can provide is to enable quick and accurate authentication of authorized users. Three areas where biometrics might prove to be beneficial are:

1. **Workstation Access:** Biometric authentication could be used at workstations in homes, offices, schools, or other locations to ensure only previously authorized users have access to the workstation.

2. **Account Access:** Biometric authentication could be used to replace passwords for access to accounts provided by Internet Service Providers (ISP).

3. **Web access:** Biometric authentication could be required for access to specific web sites, for database access, or to download data.

The advantage biometric authentication provides is the ability to require more instances of authentication in such a quick and easy manner that users are not bothered by the additional requirements. As biometric technologies mature and come into wide-scale commercial use, dealing with multiple levels of authentication or multiple instances of authentication will become less of a burden for users. An indication of the biometric industry's substantial growth and maturity is the emergence of biometric industry standards and related activities.

Biometric industry standards

Biometric industry standards are now emerging. The development of industry standards are a sign of maturity in an emerging technology such as biometrics; industry standards assure the availability of multiple sources for comparable products and of competitive products in the marketplace. Standards have a major impact on our lives. They are vital to industry, commerce, the end users, and the Enterprise[2]. Standards promote understanding between buyers and sellers and facilitate mutually beneficial commercial transactions. They spur competition, expand markets, and increase user's confidence by promoting products that prevent the sole source lock-in. In a global economy, standards have become strategic business issues[3]. Current biometric standard activities include:

- Proposed Draft ANSI/NIST-ITL 1-1999, specifying a data format for the interchange of fingerprint, facial and scar, mark, and tattoo (SMT) information [4]. This standard is a revised version of ANSI/NIST-CSL 1-1993 Standard [5]. (A revision of ANSI/NIST-ITL 1-1999 is currently in progress.)

- X9F4 Remote Access to Financial Data Working Group is developing a standard that specifies the minimum security requirements for effective management of biometrics data for the Financial Services Industry (X9.84 – Biometric Information Management and Security) [6].

- The Human Recognition Services (HRS), an extension of the Open Group's Common Data Security Architecture (CDSA) is synchronizing the development of HRS with the BioAPI Consortium effort. CDSA provides a comprehensive and coherent set of security services covering the essential components of security capability [7].

- TeleTrusT, a non-profit organization in Germany is approaching standards and analyzing biometrics in security environments. TeleTrusT formed a Biometrics Identification Systems Working Group to address these issues [8].

- B10.8, Driver License and Identification Card Tasks Group's Biometric Task Force (Sub-Group) is developing a draft technical standard for Finger Minutiae Extraction and Format for One-to-One Verification (Authentication) Systems [9].

- The Biometric Consortium, NIST, and NSA are sponsoring the development of a Common Biometric Exchange File Format (CBEFF). CBEFF is a standard format that an application can utilize to recognize what type of biometric (software and devices) is available in a system, the version number, the vendor name, etc. A common format facilitates interoperability between different biometrics technologies [10].

- In addition to technical standards, industry practices on ethics and privacy are also being developed. The International Biometric Industry Association (IBIA) is plays a crucial role in the development of these standards [11].

Biometric APIs

An Application Programming Interface (API) defines the way for a software application to communicate with a technology service or module. The API defines the application request services and handles communications to and from these services or modules. They are usually composed of a set of function calls that include data and control parameters, and defined data structures.

A Biometric API standard defines a generic way of interfacing with a broad range of biometric technologies as well as defining a common method of interfacing with a particular biometric technology. In April 2000, the **BioAPI v.1** specification was released by the BioAPI Consortium, a group of over 50 organizations including biometric vendors, major IT corporations, system integrators, and users [12].

The BioAPI is an emerging global industry specification. The BioAPI Consortium plans include submitting the specification to a standards body for further standardization as a national and/or international standard. BioAPI allows for simple integration of multiple biometrics, the use of a specific biometric technology across multiple applications, and easy substitution of biometric technologies.

BioAPI is planned as a public-domain multi-level API standard that allows for both verification and identification applications. The initial reference implementation will support Win32 operating systems.

BioAPI includes:

- simple biometric application interfaces
- standard modular access to biometric functions, algorithms, and devices
- secured and robust biometric data management and storage
- standard methods of differentiating biometric data and device types
- support for biometric identification in distributed computing environments

A key advantage of systems compliant to this specification is that applications can easily substitute one biometric technology for another without modification to the application. The BioAPI specification allows for simple integration of multiple biometrics in an application and the utilization of a specific biometric technology across multiple applications.

In addition to benefiting end-users and the Enterprise, a standard biometric API benefits system developers and the biometric industry. The common, top-level interface as defined in BioAPI v1.0 allows applications to be written once without risk of having to support different interfaces in the future. The standard also provides for flexibility of Biometric System Provider (BSP) implementation. As specified in v1.0, biometric vendors may implement a monolithic BSP, a layered BSP or special purpose objects and still comply with the standard. For those applications requiring control of biometric algorithms and devices, access to lower level functions is provided.

A common specification will hasten adoption of biometric technologies and biometric-based identification and verification solutions in multiple markets. In the near future, a large variety of BioAPI- compliant vendor biometric modules and applications are expected.

The BioAPI Consortium is currently developing a BioAPI reference implementation. A test suite for the reference implementation will follow.

Biometric Consortium

The Biometric Consortium was chartered as a Working Group on 7 December 1995 by the Facilities Protection Committee, a committee that reports to the Security Policy Board established by the President. Quoting from the Biometric Consortium charter,

> "The Consortium will serve as a Government focal point for research, development, test, evaluation, and application of biometric-based personal identification / authentication technology."

The Biometric Consortium now has over 700 members from government, industry, and academia. Over sixty different federal agencies participate in the Biometric Consortium. The main benefit of the organization is to share information about biometric technology among the members. This is done through conferences and workshops, through an electronic mail list, and through the Biometric Consortium's web site on the Internet.

Biometric Consortium World Wide Web Homepage

The Biometric Consortium web site at http://www.biometrics.org/ is open to everyone and contains a variety of information on biometric technology, research results, federal & state applications, and other topics.

Summary

There is great demand for the fast, accurate authentication that biometric systems can provide. Continued improvements in technology will bring increased performance at a lower cost. Biometric authentication, however, is not a magical solution that solves all authentication concerns. A complete systems approach that addresses a variety of security, functional, operational, and cost considerations is always necessary. The growth of biometric technology will place greater demand on both biometric system developers and users to work together to address a number of issues including privacy, testing, infrastructure, and standards. The Biometric Consortium provides a forum to facilitate this work.

Certain company names or specific biometric technologies that may have been identified in order to adequately describe the subject matter in no way imply endorsement by the Biometric Consortium, the National Institute of Standards and Technology, or the National Security Agency, nor does it imply that companies identified are the only providers of the biometric technologies referred to in this statement.

References

[1] *Biometric Consortium web site:* http://www.biometrics.org

[2] M. A. Breitenberg, Office of Standards Code and Information, Office of Product Standards Policy, National Institute of Standards and Technology, *The Abc's Of Standards-Related Activities In The United States,* NBSIR 87-3576, May 1987.

[3] Robert B. Toth, Editor, Office of Standards Services, National Institute of Standards and Technology, *Profiles of National Standards-Related Activities,* NIST SP 912.

[4] *Draft ANSI/NIST ITL 1-1999, Data Format for the Interchange of Fingerprint, Facial, & Scar, Mark & Tattoo (SMT) Information,* http://www.itl.nist.gov/iaui/894.03/fing/stand2.html

[5] *ANSI/NIST-CSL 1-1993, Data Format for the Interchange of Fingerprint Information,* http://www.itl.nist.gov/iaui/894.03/fing/stand1.html

[6] *ANSI X9,* http://www.x9.org

[7] *Open Group CDSA web site:* http://www.opengroup.org/security

[8] *Teletrust web site:* http://www.teletrust.de

[9] *AAMVAnet, Inc. Standards Development web site:* http://www.aamva.org/aamvanet/indexStandards.html

[10] *Common Biometric Exchange File Format web site:* http://www.nist.gov/cbeff

[11] *International Biometric Industry Association (IBIA) web site:* http://www.ibia.org

[12] *BioAPI Consortium web site:* http://www.bioapi.org

Fernando Podio, Co-Chair Biometric Consortium

Fernando Podio has been involved in information technology development, measurements, and standards development efforts for many years. He is a member of the National Institute of Standards and Technology (NIST), Information Technology Laboratory. He is currently the Program Manager for NIST's Biometrics and Smart Cards Program. This program is conducting research into the interoperability and performance of biometric subsystems, devices and applications, and the integration of biometrics and smart cards. Mr. Podio serves on the BioAPI Consortium Steering Committee and chairs the BioAPI Consortium's External Liaisons Working Group

Jeff Dunn, Co-Chair Biometric Consortium

Jeff Dunn is Chief of the Identification and Authentication Research Branch at the National Security Agency. This group is researching new technologies to protect access to computer systems in the Department of Defense and other critical systems. During his 20-year career at NSA, he has held a variety of program manager and management positions. He is a graduate of the Agency's Management Development Program and certified as an Acquisition Professional. Mr. Dunn has provided consultations on biometric technologies to a wide range of Government organizations.

Fernando Podio, Co-Chair Biometric Consortium

Fernando Podio has been involved in information technology development, measurements, and standards development efforts for many years. He is a member of the National Institute of Standards and Technology (NIST), Information Technology Laboratory. He is currently the Program Manager for NIST's Biometrics and Smart Cards Program. This program is conducting research into the interoperability and performance of biometric subsystems, devices and applications, and the integration of biometrics and smart cards. Mr. Podio serves on the BioAPI Consortium Steering Committee and chairs the BioAPI Consortium's External Liaisons Working Group.

Statement by
Jeffrey S. Dunn
Fernando L. Podio
Co-Chairs, Biometric Consortium
Before the
Commission on Online Child Protection
9 June 2000
Washington, D.C.

Mr. Chairman and members of the Commission, we would like to thank you for the opportunity to speak today about biometric authentication technology. We believe this Commission's interest in biometric technology is very timely. Biometric technology is one means to achieve fast, user-friendly authentication with a high level of accuracy. Recent advances in biometric technology have resulted in increased accuracy at reduced costs.

Today, to address the Commission's interest in biometrics, we would like to discuss some of the terminology used by the biometric community, highlight some of the benefits of using biometrics for authentication, and give some examples of emerging applications and standards. We would also like to explain how the Biometric Consortium[1] is bringing together technologists from government and industry.

Introduction

Biometrics are automated methods of recognizing a person based on physiological or behavioral characteristics. Examples of human traits used for biometric recognition include fingerprints, speech, face, retina, iris, handwritten signature, hand geometry, and wrist veins. During **Enrollment**, a sample of the biometric trait is taken, processed by a computer, and stored for later comparison. Biometric recognition can be used in **Identification** mode, where the biometric system identifies a person from the entire enrolled population by searching a database for a match. For example, an entire database can be searched to verify a person has not applied for entitlement benefits under two different names. This is sometimes called "one-to-many" matching. A system can also be used in **Verification** mode, where the biometric system authenticates a person's claimed identity from their previously enrolled pattern. This is also called "one-to-one" matching. In most computer access or network access environments, verification mode would be used. A user enters an account or user name as usual, but instead of entering a password, a simple touch with a finger or a glance at a camera would be enough to authenticate the user.

Biometric technologies are positioning themselves as the foundation for many highly secure identification and personal verification solutions. Areas that will benefit from biometric technologies include network security infrastructures, government IDs, secure electronic banking, investing and financial transactions, wireless communications, retail, and health and social services. Highly secure and trustworthy electronic commerce, for example, will be essential to the healthy growth of the global economy. Many biometric technology providers are already delivering biometric authentication for a variety of web-based and client/server based applications to meet these and other needs.

Advantages of Biometrics for Authentication

Using biometrics for identifying human beings offers some unique advantages. Only biometrics can identify you as you. Tokens, such as smart cards, magnetic stripe cards, photo ID cards, physical keys, and so forth, can be lost, stolen, duplicated, or left at home. Passwords can be forgotten, shared, or observed. Moreover, today's fast-paced electronic world means people are asked to remember dozens and dozens of passwords and personal identification numbers (PINs) for computer accounts, bank ATMs, e-mail accounts, wireless phones, web sites, and so forth. Biometrics hold the promise of fast, easy-to-use, accurate, reliable, and less expensive authentication for a variety of applications.

There is no one "perfect" biometric that fits all needs. All biometric systems have their own advantages and disadvantages. There are, however, some common characteristics needed to make a biometric system usable. First, the biometric must be based upon a distinguishable trait. For example, for nearly a century, law enforcement has used fingerprints to identify people. There is a great deal of scientific data supporting the idea that "no two fingerprints are alike." Technologies such as hand geometry have been used for many years and technologies such as face or iris recognition have come into widespread use. Some newer biometric methods may be just as accurate, but may require more research to establish their uniqueness.

Another key aspect is how "user-friendly" a system is. The process should be quick and easy, such as having a picture taken by a video camera, speaking into a microphone, or touching a fingerprint scanner. Low cost is important, but most implementers understand that it is not only the initial cost of the sensor or the matching software that is involved. Often, the life-cycle support cost of providing system administration and an enrollment operator can overtake the initial cost of the biometric hardware.

Biometric authentication for age verification

With the current state-of-the-art in biometric technologies, there are no means to determine the age of an individual based on a physical or behavioral characteristic. Given the wide variability of human characteristics, it seems unlikely any that such technologies will be available in the future.

The most likely benefit biometric technologies can provide is to enable quick and accurate authentication of authorized users. Three areas where biometrics might prove to be beneficial are:

1. **Workstation Access:** Biometric authentication could be used at workstations in homes, offices, schools, or other locations to ensure only previously authorized users have access to the workstation.

2. **Account Access:** Biometric authentication could be used to replace passwords for access to accounts provided by Internet Service Providers (ISP).

3. **Web access:** Biometric authentication could be required for access to specific web sites, for database access, or to download data.

The advantage biometric authentication provides is the ability to require more instances of authentication in such a quick and easy manner that users are not bothered by the additional requirements. As biometric technologies mature and come into wide-scale commercial use, dealing with multiple levels of authentication or multiple instances of authentication will become less of a burden for users. An indication of the biometric industry's substantial growth and maturity is the emergence of biometric industry standards and related activities.

Biometric industry standards

Biometric industry standards are now emerging. The development of industry standards are a sign of maturity in an emerging technology such as biometrics; industry standards assure the availability of multiple sources for comparable products and of competitive products in the marketplace. Standards have a major impact on our lives. They are vital to industry, commerce, the end users, and the Enterprise[2]. Standards promote understanding between buyers and sellers and facilitate mutually beneficial commercial transactions. They spur competition, expand markets, and increase user's confidence by promoting products that prevent the sole source lock-in. In a global economy, standards have become strategic business issues[3]. Current biometric standard activities include:

- ♣ Proposed Draft ANSI/NIST-ITL 1-1999, specifying a data format for the interchange of fingerprint, facial and scar, mark, and tattoo (SMT) information [4]. This standard is a revised version of ANSI/NIST-CSL 1-1993 Standard [5]. (A revision of ANSI/NIST-ITL 1-1999 is currently in progress.)

- ♣ X9F4 Remote Access to Financial Data Working Group is developing a standard that specifies the minimum security requirements for effective management of biometrics data for the Financial Services Industry (X9.84 – Biometric Information Management and Security) [6].

- The Human Recognition Services (HRS), an extension of the Open Group's Common Data Security Architecture (CDSA) is synchronizing the development of HRS with the BioAPI Consortium effort. CDSA provides a comprehensive and coherent set of security services covering the essential components of security capability [7].

- TeleTrusT, a non-profit organization in Germany is approaching standards and analyzing biometrics in security environments. TeleTrusT formed a Biometrics Identification Systems Working Group to address these issues [8].

- B10.8, Driver License and Identification Card Tasks Group's Biometric Task Force (Sub-Group) is developing a draft technical standard for Finger Minutiae Extraction and Format for One-to-One Verification (Authentication) Systems [9].

- The Biometric Consortium, NIST, and NSA are sponsoring the development of a Common Biometric Exchange File Format (CBEFF). CBEFF is a standard format that an application can utilize to recognize what type of biometric (software and devices) is available in a system, the version number, the vendor name, etc. A common format facilitates interoperability between different biometrics technologies [10].

- In addition to technical standards, industry practices on ethics and privacy are also being developed. The International Biometric Industry Association (IBIA) is plays a crucial role in the development of these standards [11].

Biometric APIs

An Application Programming Interface (API) defines the way for a software application to communicate with a technology service or module. The API defines the application request services and handles communications to and from these services or modules. They are usually composed of a set of function calls that include data and control parameters, and defined data structures.

A Biometric API standard defines a generic way of interfacing with a broad range of biometric technologies as well as defining a common method of interfacing with a particular biometric technology. In April 2000, the **BioAPI v.1** specification was released by the BioAPI Consortium, a group of over 50 organizations including biometric vendors, major IT corporations, system integrators, and users [12].

The BioAPI is an emerging global industry specification. The BioAPI Consortium plans include submitting the specification to a standards body for further standardization as a national and/or international standard. BioAPI allows for simple integration of multiple biometrics, the use of a specific biometric technology across multiple applications, and easy substitution of biometric technologies.

BioAPI is planned as a public-domain multi-level API standard that allows for both verification and identification applications. The initial reference implementation will support Win32 operating systems.

BioAPI includes:

- simple biometric application interfaces
- standard modular access to biometric functions, algorithms, and devices
- secured and robust biometric data management and storage
- standard methods of differentiating biometric data and device types
- support for biometric identification in distributed computing environments

A key advantage of systems compliant to this specification is that applications can easily substitute one biometric technology for another without modification to the application. The BioAPI specification allows for simple integration of multiple biometrics in an application and the utilization of a specific biometric technology across multiple applications.

In addition to benefiting end-users and the Enterprise, a standard biometric API benefits system developers and the biometric industry. The common, top-level interface as defined in BioAPI v1.0 allows applications to be written once without risk of having to support different interfaces in the future. The standard also provides for flexibility of Biometric System Provider (BSP) implementation. As specified in v1.0, biometric vendors may implement a monolithic BSP, a layered BSP or special purpose objects and still comply with the standard. For those applications requiring control of biometric algorithms and devices, access to lower level functions is provided.

A common specification will hasten adoption of biometric technologies and biometric-based identification and verification solutions in multiple markets. In the near future, a large variety of BioAPI- compliant vendor biometric modules and applications are expected.

The BioAPI Consortium is currently developing a BioAPI reference implementation. A test suite for the reference implementation will follow.

Biometric Consortium

The Biometric Consortium was chartered as a Working Group on 7 December 1995 by the Facilities Protection Committee, a committee that reports to the Security Policy Board established by the President. Quoting from the Biometric Consortium charter,

> "The Consortium will serve as a Government focal point for research, development, test, evaluation, and application of biometric-based personal identification / authentication technology."

The Biometric Consortium now has over 700 members from government, industry, and academia. Over sixty different federal agencies participate in the Biometric Consortium. The main benefit of the organization is to share information about biometric technology among the members. This is done through conferences and workshops, through an electronic mail list, and through the Biometric Consortium's web site on the Internet.

Biometric Consortium World Wide Web Homepage

The Biometric Consortium web site at http://www.biometrics.org/ is open to everyone and contains a variety of information on biometric technology, research results, federal & state applications, and other topics.

Summary

There is great demand for the fast, accurate authentication that biometric systems can provide. Continued improvements in technology will bring increased performance at a lower cost. Biometric authentication, however, is not a magical solution that solves all authentication concerns. A complete systems approach that addresses a variety of security, functional, operational, and cost considerations is always necessary. The growth of biometric technology will place greater demand on both biometric system developers and users to work together to address a number of issues including privacy, testing, infrastructure, and standards. The Biometric Consortium provides a forum to facilitate this work.

Certain company names or specific biometric technologies that may have been identified in order to adequately describe the subject matter in no way imply endorsement by the Biometric Consortium, the National Institute of Standards and Technology, or the National Security Agency, nor does it imply that companies identified are the only providers of the biometric technologies referred to in this statement.

References

[1] *Biometric Consortium web site:* http://www.biometrics.org

[2] M. A. Breitenberg, Office of Standards Code and Information, Office of Product Standards Policy, National Institute of Standards and Technology, *The Abc's Of Standards-Related Activities In The United States,* NBSIR 87-3576, May 1987.

[3] Robert B. Toth, Editor, Office of Standards Services, National Institute of Standards and Technology, *Profiles of National Standards-Related Activities,* NIST SP 912.

[4*] Draft ANSI/NIST ITL 1-1999, Data Format for the Interchange of Fingerprint, Facial, & Scar, Mark & Tattoo (SMT) Information,* http://www.itl.nist.gov/iaui/894.03/fing/stand2.html

[5] *ANSI/NIST-CSL 1-1993, Data Format for the Interchange of Fingerprint Information,* http://www.itl.nist.gov/iaui/894.03/fing/stand1.html

[6] *ANSI X9,* http://www.x9.org

[7] *Open Group CDSA web site:* http://www.opengroup.org/security

[8] *Teletrust web site:* http://www.teletrust.de

[9] *AAMVAnet, Inc. Standards Development web site:* http://www.aamva.org/aamvanet/indexStandards.html

[10] *Common Biometric Exchange File Format web site:* http://www.nist.gov/cbeff

[11] *International Biometric Industry Association (IBIA) web site:* http://www.ibia.org

[12] *BioAPI Consortium web site:* http://www.bioapi.org

Fernando Podio, Co-Chair Biometric Consortium

Fernando Podio has been involved in information technology development, measurements, and standards development efforts for many years. He is a member of the National Institute of Standards and Technology (NIST), Information Technology Laboratory. He is currently the Program Manager for NIST's Biometrics and Smart Cards Program. This program is conducting research into the interoperability and performance of biometric subsystems, devices and applications, and the integration of biometrics and smart cards. Mr. Podio serves on the BioAPI Consortium Steering Committee and chairs the BioAPI Consortium's External Liaisons Working Group

Jeff Dunn, Co-Chair Biometric Consortium

Jeff Dunn is Chief of the Identification and Authentication Research Branch at the National Security Agency. This group is researching new technologies to protect access to computer systems in the Department of Defense and other critical systems. During his 20-year career at NSA, he has held a variety of program manager and management positions. He is a graduate of the Agency's Management Development Program and certified as an Acquisition Professional. Mr. Dunn has provided consultations on biometric technologies to a wide range of Government organizations.

DAVID SOBEL
GENERAL COUNSEL, EPIC

David L. Sobel is General Counsel to the Electronic Privacy Information Center in Washington, DC, where he has litigated numerous cases involving Internet and privacy policy. Mr. Sobel served as co-counsel in ACLU v. Reno, the constitutional challenge to the Communications Decency Act favorably decided by the U.S. Supreme Court in June 1997. He currently serves as co-counsel in ACLU v. Reno II, the pending challenge to the Child Online Protection Act. Mr. Sobel coordinates the Internet Free Expression Alliance, a coalition of more than two dozen organizations committed to the continuation of the Internet as a forum for open, diverse and unimpeded expression. He also serves on the steering committee of the Free Expression Network.

Mr. Sobel has a longstanding interest in privacy, civil liberties, national security and information access issues and has written and spoken on these issues frequently since 1980. He is a graduate of the University of Michigan and the University of Florida College of Law. He is a member of the Bars of Florida, the District of Columbia, the U.S. Supreme Court and several federal Courts of Appeals.

*** Please Note New Address and Phone Numbers ***

....

David L. Sobel, General Counsel * +1 202 483 1140 (tel)
Electronic Privacy Information Center * +1 202 483 1248 (fax)
1718 Connecticut Ave., N.W. Suite 200 * sobel@epic.org
Washington, DC 20009 USA * http://www.epic.org

Statement of
David L. Sobel
General Counsel
Electronic Privacy Information Center

Before the
Commission on Online Child Protection

June 9, 2000
Washington, DC

Mr. Chairman and Members of the Commission:

Thank you for providing me with the opportunity to appear before the Commission to address the privacy implications of age verification technologies that might be used to restrict access to certain material on the Internet. The Electronic Privacy Information Center (EPIC), as an organization committed to the protection of both privacy rights and free expression, has a longstanding interest in this issue and has participated in relevant legislative and judicial proceedings since its inception in 1994. We also co-founded and coordinate the Internet Free Expression Alliance (www.ifea.net), a coalition of more than two dozen organizations committed to the continuation of the Internet as a forum for open, diverse and unimpeded expression with particular emphasis on both legal and technological impediments to free expression.

As an initial matter, I note that the Commission has invited me to discuss the rather limited question of whether age verification systems pose threats to personal privacy. While I welcome the opportunity to address that issue, my testimony would be incomplete if I did say a word about the underlying premise of the Commission's inquiry, namely "to identify technological or other methods that . . . will help reduce access by minors to material that is harmful to minors on the Internet." Given the inherent subjectivity of terms such as "harmful to minors" or "indecent," I believe that efforts to mandate restrictions on access to such material are prohibited by the First Amendment, particularly in a medium like the Internet, which makes content available in every community in the nation. For that reason, EPIC participated as plaintiff and co-counsel in the constitutional challenge to the Communications Decency Act and is currently acting in a similar capacity in the pending challenge to the criminal provisions of the Child Online Protection Act (COPA). Every federal judge (including the Justices of the Supreme Court) who has considered the issue has agreed that content-based restrictions on Internet "indecent" or "harmful to minors" speech are unconstitutional.

First Amendment considerations are an important aspect of my testimony today, because I believe the privacy issues we are discussing are inseparable from the free speech issues. Any requirement that Internet users identify themselves in some way (or even take additional steps to establish that they are entitled to receive the information they seek) as a condition of access to online content necessarily chills free speech. The courts have recognized that the exercise of First Amendment rights may not be conditioned upon a surrender of personal privacy. For instance, a federal appeals court invalidated a state's requirement that citizens provide their Social Security numbers when registering to vote, finding that such requirements "compel a would-be voter . . . to consent to the possibility of a profound invasion of privacy when exercising the fundamental right to vote."[1] Likewise, mandated age verification systems impose a similar condition on an adult's right to access information on the Internet. Such requirements also infringe on the First Amendment right to communicate anonymously. As the Supreme Court stated in *McIntyre v. Ohio Elections Commission*, anonymity "exemplifies the purpose behind the Bill of Rights, and of the First Amendment in particular: to protect unpopular individuals from retaliation -- and their ideas from suppression -- at the hand of an intolerant society."[2]

The privacy impacts of age verification -- and therefore the free speech implications -- are felt by both consumers and providers of online content. From a consumer perspective, a new regime for the collection of personal data in the name of "child online protection" would impose yet another burden on the privacy of Internet users. The American people, when they go online, are already acutely aware of the fact that they are being over-monitored and over-profiled. Polling results consistently show that many Americans are "concerned" or "very concerned" about the loss of privacy, particularly with regard to commercial transactions that take place over the Internet.[3] One recent poll has indicated that the "loss of personal privacy" is the number one concern facing the United States in the twenty-first century. These results are not surprising when an Internet advertising firm such as DoubleClick reportedly has compiled approximately 100 million online user profiles to date.

---

[1] *Greidinger v. Davis*, 988 F.2d 1344, 1354 (4th Cir. 1993).

[2] 115 S. Ct. 1511, 1524 (1995) (striking down an Ohio statute prohibiting anonymous distribution of campaign literature). *See also Lamont v. Postmaster General*, 381 U.S. 301, 307 (1965) (finding unconstitutional a requirement that recipients of communist literature notify the post office that they wish to receive it); *Talley v. California*, 362 U.S. 60, 64-65 (1960) (declaring unconstitutional a California ordinance that prohibited the distribution of anonymous handbills); *ACLU of Georgia v. Miller*, 977 F. Supp. 1228 (N.D. Ga. 1997) (striking down Georgia statute that would have made it a crime for Internet users to "falsely identify" themselves online).

[3] A recent poll conducted by Newsweek asked respondents how they would feel about a Web site that "tracked your movements when you browsed the site, but didn't tie that information to your name or real-world identity." Even that relatively anonymous kind of tracking led 28 percent to say they would feel "not very comfortable" and 35 percent to feel "not at all comfortable." If the site "merged your browsing habits and shopping

Given the public concern over online privacy, it seems apparent that age verification requirements will deter most adults from accessing restricted content, because Web users are increasingly unwilling to provide identifying information in order to gain access to online content. Web users who wish to access sensitive or controversial information are even less likely to register to receive it.[4] The district court recognized this fact when it found COPA to be unconstitutional, noting that "the implementation of credit card or adult verification screens in front of material that is harmful to minors may deter users from accessing such materials."[5] Indeed, the uncontroverted evidence presented to the court established that COPA's age verification requirements would prevent or deter Web users from accessing a wide range of constitutionally protected speech.[6]

There is little doubt that all effective age verification technologies require consumers, at some stage of the verification process, to divulge personally identifiable information,

---

patterns into a profile that was linked to your real name and identity," 21 percent would feel "not very comfortable" and 68 percent "not at all comfortable." http://www.businessweek.com/2000/00_12/b3673010.htm

[4] In a related context, the Supreme Court has recognized that identification requirements can have a chilling effect on access to sexually-explicit material. In *Denver Area Educ. Telecomms. Consortium, Inc. v. FCC*, 518 U.S. 727 (1996), the Court struck down a statutory requirement that viewers provide written notice to cable operators to obtain access to certain sexually oriented programs because the requirement "restrict[s] viewing by subscribers who fear for their reputations should the operator, advertently or inadvertently, disclose the list of those who wish to watch the . . . channel." 518 U.S. at 754. In considering the precursor to COPA, the Supreme Court found that the credit card and adult access code requirements of the CDA would also unconstitutionally inhibit adult Web browsers. *Reno v. ACLU*, 521 U.S. at 857 n.23 ("There is evidence suggesting that adult users, particularly casual Web browsers, would be discouraged from retrieving information that required use of a credit card or password.").

[5] *American Civil Liberties Union v. Reno* ("*ACLU II*"), 31 F. Supp.2d 473, 495 (E.D. Pa. 1999).

[6] The evidence also showed that Internet users would be deterred by adult access code services that cater to the pornography industry, and would not want to affiliate with such services in order to gain access to material deemed to be "harmful to minors."

whether a credit card number, driver's license, birth certificate or other documentation. The Adult Check system, for instance, claims that it has the ability to verify independently the age of an applicant and, in order to prevent "password sharing," resorts to "originating IP address verification." While some of these technologies (such as some digital certificate systems) are less invasive than others, they all require the consumer to provide personal data to a third party.[7] On a truly voluntary basis, some consumers may choose to avail themselves of such technologies in order to conduct online transactions, and when carefully implemented they can play a useful role in facilitating electronic commerce. But any governmental mandate to obtain and use such an age verifier as a condition of access to information suffers from the constitutional defects that I have discussed.

As I have noted, the use of age verification systems impacts providers of online content as well as consumers. Given the apprehension that many consumers have about obtaining an adult ID or password, content providers who would be required to impose such requirements as a condition of access to their Web sites will suffer a loss of traffic and, consequently, revenue. Indeed, the inhibiting effect of such systems formed the basis for the district court's discussion of the issue when it considered the constitutionality of COPA:

> Evidence presented to this Court is likely to establish at trial that the implementation of credit card or adult verification screens in front of material that is harmful to minors may deter users from accessing such materials and that the loss of users of such material may affect the speakers' economic ability to provide such communications. The plaintiffs are likely to establish at trial that under COPA, Web site operators and content providers may feel an economic disincentive to engage in communications that are or may be considered to be harmful to minors and thus, may self-censor the content of their sites.[8]

The court's finding underscores the clear relationship between the privacy and free speech aspects of age verification requirements; one simply cannot be separated from the other. For that reason, such requirements would introduce a troubling new component into the Internet's architecture, one that would hasten the demise of both personal privacy and freedom of expression. I submit that such a result is not in the long-term interests of the emerging online industry or of an American public that is increasingly turning to this medium as a vital source of information and entertainment. Rather than focus on approaches that seek to block access to information and compromise privacy, I strongly urge both the Commission and Congress to emphasis and support educational initiatives that will help young people learn to responsibly and safely navigate this exciting and enriching medium.

---

[7] Digital certification technologies can lessen the privacy and First Amendment implications of age verification systems, but not remove them entirely. Such approaches can separate personal identity from a particular certified characteristic; age, for instance. But they still impose upon the user the burden of providing information to the third party certificate issuer, a burden that raises constitutional problems when imposed as a condition of accessing a particular category of information.

[8] *ACLU II*, 31 F. Supp.2d at 495.

COPA Commission

Information and Resources About the
Commission on Online Child Protection (COPA)
Hosted by the Congressional Internet Caucus Advisory Committee

Additional Testimony for June 8-9 Hearings

The following organizations submitted written testimony to the Commission.

- Laith Alsarraf, President, Chief Executive Officer and co-founder of Cybernet Ventures, Inc. (.pdf)
- Browsesafe (.pdf)
- Enough is Enough (.pdf)
- Flying Crocodile (.pdf)
- Internet Corporation for Assigned Names and Numbers (ICANN) (.html)

[Home] [Final Report] [About this Site] [FAQ] [The Commission] [Press Room]
[Meetings and Hearings] [Research Papers] [Privacy Policy]

webmaster@copacommission.org / Copyright © 2000

Prepared Testimony of
Laith P. Alsarraf
President and CEO of
Cybernet Ventures, Inc.

BEFORE THE COMMISSION ON ONLINE CHILD PROTECTION

INTRODUCTION

On behalf of Cybernet Ventures, Inc. I am pleased to have this opportunity to testify before the Commission on Online Child Protection. My name is Laith Alsarraf and I am the President, Chief Executive Officer and co-founder of Cybernet Ventures, Inc. By way of background and history, I was born in Ontario Canada in 1969. Both of my parents are doctors and following in the family tradition, I attended UCLA as a pre-med student. While in college, I also worked as a contract programmer and website designer. The success of these computer oriented ventures pushed my formal education to the sidelines and I formed a company that soon required my full time attention. I now have several corporations each providing technology and development services in a wide variety of areas. Our flagship company is Cybernet Ventures, Inc., which provides the age verification service Adult Check®.

In 1996 the Congress of the United States passed into law the Telecommunications Reform Act ("TRA"), which among other things addressed certain issues dealing with access to the internet by minors. The portion of the TRA, which dealt with internet content and access, was the Communications Decency Act ("CDA"). The original CDA created a 'safe harbor' from prosecution for those websites that provide content that might be considered indecent or harmful to minors provided that those websites took reasonable steps to prevent access by minors. In response to the first CDA, Cybernet Ventures, Inc. was formed to provide age verification services ("avs") to websites, which provide content that may be harmful to minors. Cybernet Ventures, Inc. provides avs through Adult Check®. Since its inception, Cybernet Ventures, Inc. has experienced unprecedented growth and success, and the Adult Check® age verification service is, by a significant margin, the largest and most widely used avs.

Currently the "avs" Adult Check® is used by over 200,000 websites. The number is growing steadily. Adult Check® has enjoyed widespread acceptance and recognition. Since I testified before the Subcommittee on Telecommunications, Trade and Consumer Protection in support of COPA, Adult Check® and Adult Check Gold® have received Federal service mark registration. In addition, we have made great strides in technology to provide more effective age verification services to address some of the concerns and objections raised by COPA opponents in CDAII.

We have invested considerable resources in the development of new, comprehensive programs that have, and I am quite certain, will continue to keep Adult Check® on the forefront of the industry. Of course to keep our competitive advantage, we assiduously guard our intellectual property and, as such, many of our systems are proprietary. I am prepared to discuss, in general terms, the many breakthroughs that make Adult Check® the premier avs.

AGE VERIFICATION SERVICES

Age verification software is a script embedded into a webpage which can be implemented by a website owner in minutes. There is no charge for the service to the website owner. The script is free and to install it requires no programming or technical expertise beyond that required to put up a website. This script can be placed at the entrance or any other area of a site which may contain material harmful to minors preventing further access or exposure of the website's content by requiring a personal identification number ("PIN"), which is only available to adults. If a consumer does not have a PIN, a link is provided for them to obtain one from the avs associated with that site. Consumers may obtain a PIN instantly by submitting an application to an age verification system. The credit card and other information submitted by a consumer are verified by a proprietary fraud and age verification system to determine its validity and the actual age of the applicant. If the information is deemed to be valid and the applicant is at least 18 years of age, a working PIN is issued. The process of verifying the information submitted generally takes from 5 to 10 seconds.

Cybernet Ventures, Inc. does not sponsor or display any content. The services provided by Cybernet Ventures, Inc. are limited to age verification and the assignment of personal identification numbers ("PIN"). A consumer applies for a PIN online or by fax. The application is encrypted, submitted and processed through a proprietary software system that determines the validity of the credit card and the age of the applicant. The software program is designed to also provide risk scoring, fraud and chargeback control. Once approved, the consumer can use his (or her) PIN to access over two hundred thousand websites. The website is assured that any visitor has been 'age verified' by Adult Check®. The consumer is charged a nominal fee of $19.95 for a one year 'membership.'

Although an avs is not completely foolproof, since 1998 many technological innovations have made Adult Check® extremely effective. The two most common criticisms are: 1) once a PIN is issued it can be shared with thousands of potential users, many of whom may be minors by posting it on the internet; and 2) minors have access to credit cards, some with their parents permission, some without. Adult Check® now has the ability to verify the age of an applicant, even minors with a valid credit card. This technology makes it possible for the Adult Check® system to effectively screen out minors. PINs are not issued to anyone under the age of 18 on the date of the application.

Cybernet Ventures, Inc. has already developed several proprietary methods to detect password sharing. Velocity checks, relational database management, originating IP address verification and other fraud controls have been designed and are constantly being improved. For example, PINs that have been distributed and are being used by multiple individuals are invalidated within minutes by Cybernet Ventures' proprietary PIN protection software. Significant resources have been and will be dedicated to maintain, develop and implement more effective technologies and to develop new and better methods to prevent fraudulent use of PINs.

Adult Check® provides a high level of customer service accessible via a toll free telephone number or e-mail 24 hours a day, 7 days a week. If a parent contacts Adult Check® concerning an unauthorized use of their credit card, a credit is issued to their account, the password is invalidated and the card number is blocked.

Stolen credit cards, bogus card numbers, numbers posted on the internet and other fraudulent credit card transactions are detected by the use of several systems. Each transaction is authorized or declined 'scrubbed' through our proprietary age verification and fraud protection programs and then authorized by the credit card company (e.g. VISA®, Mastercard®, and American Express®). Even if the credit card is determined to be valid, the transaction is subjected to other checks to determine the validity of that particular transaction. These other checks are proprietary and the systems and programs are protected trade secrets with patents pending. All of these efforts are brought to bear on the issue of validity to protect consumers and prevent unauthorized use of credit cards. Most importantly, every effort is made to prevent minors from accessing websites that contain content that may not be suitable for them.

Currently Adult Check® is used by a significant percentage of adult content websites on the internet. In addition, Adult Check® is also used to restrict access to numerous sites that contain non-sexual content that may also be considered harmful to or inappropriate for minors. Even though the CDA was overturned and the enforcement of COPA was, at least temporarily, enjoined, many website owners continue to use Adult Check® as a responsible approach to content accessibility. Adult Check® is free to websites, extremely simple to implement and highly effective. Adult Check® is easy to use, and inexpensive for the customer. The avs model has been widely accepted among website owners and consumers because of its effectiveness, ease of implementation and use, and its nominal cost. The consumer pays a nominal fee of $19.95 for access to over 200,000 websites for a year and the website owner pays nothing.

From a consumer standpoint, an avs is superior to direct credit card verification at each site. Because of Adult Check's® reputation for being secure, responsible, independent and easy to use, consumers have confidence in providing credit card information to Adult Check®. In addition, Adult Check® has no interest in the consumer beyond the service of age verification. We do not contact them, sell them additional services or trade in consumer information. The credit card information is strictly confidential and is not shared, sold or disseminated. All transactions are encrypted and stored behind an elaborate firewall.

Adult Check® is "age verification at website based on relationship established with a third party site." At present, and as discussed above, it is an effective and successful means of keeping minors off of sites that are unsuitable to them on a voluntary basis. Adult Check® webmasters use a password screen and adult verification identifier to restrict access to adult content sections of a given site.

Adult Check® actually verifies the age of the consumer and determines, within a high degree of probability, the accuracy of the application information. If invalid information is detected, the system returns an invalid information message that requires further input. The system is dynamic and will ask the user to input information that is relevant to the specific inconsistencies detected. It is extremely difficult and in almost all cases impossible, for a minor or non-authorized 'customer' to guess all the required information within the time constraints of the system. In addition, the credit card companies have adopted CVV2 technology which makes it almost impossible to use a credit card number without having the actual credit card in hand. Adult Check® is fully CVV2 compliant.

The Adult Check® system is also dynamic. As technology changes, so does the system. The Adult Check® system is adaptable to many e-commerce applications and, in addition to basic age verification; it can be used, in a wide variety of web businesses.

The Adult Check® system is widely available, accepted and used by consumers and website owners. Because website owners place the Adult Check® script on their websites, end users encounter the system only when looking to obtain access to adult sites. The cost is minimal, starting at $19.95 for a year for access to thousands of sites.

There is no cost to the website owner to become an Adult Check® webmaster. In fact, webmasters are incented to use the system. A webmaster receives a commission for every end user that signs up for a PIN through his or her site.

As discussed above, the Adult Check® system makes it very difficult for a minor to obtain an Adult Check PIN and because of the effectiveness of the Adult Check® system, its use by websites should be a defense to a COPA charge.

CONCLUSION

Age verification services generally and Adult Check® specifically provide an effective, content neutral method to protect minors from accessing harmful or indecent materials on the internet. Using current technology and a successful business model Adult Check® allows a free flow of ideas and constitutionally protected speech to course through the internet without censorship and unreasonable intrusion. Recent developments in technology have procedural safeguards to reasonably accomplish the intended goal of protecting children without an overly broad or over-reaching approach. The Adult Check® system is the least restrictive, least intrusive method of restricting access to content that requires minimal cost, and no parental technical expertise and intervention: it does not judge content; does not inhibit free speech; and, it does not prevent access to any ideas, word, thoughts or expressions. With the new technological developments, Adult Check® can verify the age of an applicant, even a minor who validly possesses a credit card. Adult Check® prevents minors from accessing materials on the internet not suitable and potentially harmful.

RESPECTFULLY SUBMITTED

Laith Alsarraf, President and CEO
Cybernet Ventures, Inc.
The Adult Check® System

PlanetGood by Browsesafe.com

- How often is the resource used? ***PlanetGood is used on a daily basis by a wide number of customers.***
- How often is the resource updated? ***The PlanetGood Resource is updated by the minute.***
- In what particular ways does the resource assist parents? ***PlanetGood goes to each website and characterizes the website according to 37 characteristics. The Parent sets up separate accounts for children to use that gives them access according to what the Parent wants them to see.***
- Is there any data regarding satisfaction of those who use the resource? ***Yes, Parents like the freedom to search the web without filters, and the peace of mind they get from children surfing the net safely.***
- How is the resource marketed or promoted? ***Planet Good is available through Priceline right now. It can be downloaded from Browsesafe.com directly for 15 day free trial. It also is available through Cybercross.net and several Internet providers.***
- Does the resource help prevent access by children to web sites with materials harmful to minors? ***Absolutely! PlanetGood prevents children from having access to the bad stuff by the characters we give it. They do not decide what the child can see. The parents have that right. Pornography is already filtered. If a child comes to site that has not been reviewed, they must submit it to the reviewers before they can see it.***
- Does the resource help prevent problems associated with incoming email? ***Absolutely! PlanetGood has some emails set in the default that children cannot have access without the parents; it also helps limit access to certain sites that offer free mail services by characterizing the site.***
- What percentage of those who use the resource go on to select and use specific tools it identifies? ***PlanetGood is a specific tool to administer a safer Internet. Everyone who has it installed and runs with it is using the tool.***
- Does the resource provide assistance to companies offering blocking or filtering services? ***Browsafe.com owns PlanetGood. The rights and privileges are protected by copyright. Purchase is optional.***
- What could be done to make it easier to locate the resource? ***The awareness that the product exists would make it more accessible for Parents to find.***
- What if anything could be done to increase usage of the resource? ***The awareness that the product exists would make it more accessible for Parents to use.***
-
- What if anything could be done to make the resource more effective? ***Increasing the size of our database for sites reviewed will make PlanetGood more effective. Every day that database increases.***
- Should the availability of the resource be considered to provide a defense to prosecution under COPA? ***PlanetGood can be used as a preventative measure to keep children away from sites that are questionable. Sites that contain Adult content can be monitored through addressing the Attributes that are assigned.***
- Does the resource provide any assistance to law enforcement? ***Due to the nature of PlanetGood, assistance to law enforcement is not involved in the product.***

- Does use of the resource create any data that implicates privacy rights? ***Absolutely not! The PlanetGood product does not track or infringe on privacy rights.***
- Does the existence of the resource raise any first amendment issues? ***No! In fact, PlanetGood by Browsesafe.com completely utilizes the first amendment by allowing parent's the choice of what their children see and don't see.***
- Does the availability of the resource increase the likelihood that parents who wish to do so will be able to restrict access by their children to materials harmful to minors? ***Parents who want a safer Internet for their children are PlanetGood's purpose.***
- What other information might usefully be included in a common resource? ***In a common resource, there is a need for product ratings, operational specifications, and technical specifications of each product.***
- Are there legal or other barriers to the sharing of useful information via this common resource? ***PlanetGood can track how many users go to particular websites in statistical terms without information of individuals being released.***
- Is there a business model that assures continued availability and enhancement of this common resource? ***Yes, Browsesafe.com continually updates sites and software to provide easy safe Internet access.***
- Would governmental action to subsidize or regulate this common resource raise first amendment or other issues? ***At this time, it does not appear to cause issues. However, BrowseSafe believes Parents should have the ultimate decision in what the child is exposed to.***
- What reason is there to believe that any problems in parental adoption of various technologies or methods or restraining access by their children are due to lack of information or other tools that would be provided by a common resource? ***All other tools we know of provide a compromised solution.***
- Could the resource be made more readily available or more easily used if it were tied into the browser in some more direct way (e.g., as an always-visible icon)? Do you have reason to believe that the Internet industry would support creation of something like an always-visible icon? Should the government require browsers or operating system software to include such an icon? ***PlanetGood already works with Netscape, IE, and other browsers to provide a safer net. The icon does not change in the browser because PG works with the browser as it runs.***
- Should web sites with material harmful to minors be required to link to such a common resource? ***No linkages are necessary; PlanetGood would characterize the site regardless. It does not determine what is bad/good. It allows the Parents to choose. Pornography is taken out through PG product.***
- Should restrictions on unsolicited email be relaxed with respect to messages advertising such a resource? ***An appropriate e-mail message would have value to nearly all Internet users.***
- What evidence is there regarding the extent to which Internet using parents are actually aware of the resource? ***The PlanetGood Product has little awareness in the market at this time. Due to the nature of the concern in the Internet accessibility of children, PG's awareness will increase in the media and on the net.***
- If the resource lists safe sites, are those listings accurate and up to date? ***Yes, every site has its characteristics done to a standard, and the Parents get to choose what is safe. PlanetGood also reevaluates sites to ensure it has not changed.***

- What percentage of parents wants to limit their children's access to only safe sites listed in such a resource? ***There have been very few Parents who know what's out there that have not been interested in preventing children from having access to it all.***
- Is there a technological means of assuring that a child only has access to the listed safe sites? ***Yes, the technology used by PlanetGood does keep the Bad out and let's what the parents want the child to see in.***
- What kinds of useful material would be rendered unavailable to children if only listed safe sites could be visited? ***PlanetGood can give access to any site with personal permission. Therefore, No valuable information is "unavailable"***

Establishment of a [top level] domain name for any material that is harmful to minors

- ***Whether a site has a [top level] domain name or not does not influence the PlanetGood Product. PlanetGood characterizes all sites that are submitted to the proxy. It categorizes the site according to the Attributes the site has. If the site changes, the characteristics change. PlanetGood again allows the Parents the choice of what the child has access to on the Internet. If a site changes from a [top level] domain to an education site, PlanetGood reevaluates the characteristics.***

Age Verification systems

PlanetGood sets up accounts according to age ranges. There are currently 5 age ranges for accounts: 0-8, 8-13, 13-15, 15-18, and 18 up. It opens an account for a child according to age range with default characteristics. These characteristics can then be accessed and changed according to the Parent's belief system.

To: Commission on Online Child Protection

June 13, 2000

Submitted By: Enough Is Enough
Contact: Monique Nelson (714) 435-9056 - e-mail: eieca@enough.org

Comments on First Hearing Subjects

Enough Is Enough's programs and resources are directed towards ***Making the Internet Safe for Children and Families.***

Through the marvels of the Internet, vast new worlds of opportunity have been opened to this generation. Today the children of this country have access to information, which they could only have dreamed of in the past. The Internet is one of the most positive educational tools developed in our century. In the last few years it has begun to revolutionize the way we communicate, entertain, do business and live our lives. *It is fun, fascinating, and it is the future. Unfortunately, it has been misused and can seriously threaten the safety of our children.*

Our Mission: Enough Is Enough was launched in 1992 to educate the American people about the importance of protecting children from the harms of predators and pornography, and the link to sexual violence. With technology making computers affordable for millions of homes, schools and public libraries, America is now experiencing the fastest spreading and most dangerous pornography known to our society today… on the Internet. *There are two primary threats: children's easy access to pornography and predator's easy access to children.*

During the past eight years, the staff of Enough Is Enough has educated members of Congress, media, schools and libraries about the issue of computer pornography. We have initiated and sustained on-going dialogs with the technology community stressing corporate responsibility to protect children using their services. As a result, Enough Is Enough is now recognized as a leader on this issue and as a bridge builder between these entities, who see us seeking reasonable solutions that protect children and our Constitutional freedoms.

Enough Is Enough is an independent, non-partisan, non-profit 501(c)(3) organization. Because we focus on protecting children from pornography, we enjoy a diverse base of support that includes individuals from various political, social, ethnic and religious backgrounds. Sources of financial support include foundation grants, fundraising events, and corporate and individual contributions.

Addressing a Serious Problem in Our Society: Early in 1994, the staff of Enough Is Enough became aware of the pornographers' new method of delivery – the Internet. On the Internet, at home, at school, or in public libraries, children have access to some of the most harmful, hard core pornography available. Their lives are forever changed by the images they encounter.

The statistics are shocking:

- "Web surfers spent $970 million on access to adult-content sites in 1998 and that is expected to rise to more than $3 billion by 2003." (U.S. News & World Report, 3/27/2000)
- "There are now 40,000 porn sites on the World Wide Web and probably thousands more. No one has been able to count them all." (U.S. News and World Report, 3/27/2000)
- According to Nielson NetRatings, 17.5 million surfers visited porn sites from their homes in January; a 40% increase compared with 4 months earlier.
- Time Magazine predicted that 42 million children will be online by the year 2005, most will be unsupervised.

For the first time in history, child pornography, obscenity and harmful to minors material, which previously were not available on the open market, have become fair game to anyone who wants it – ***and often to those who don't want it.*** Families now face the prospect of having it enter their children's bedroom, school or library via the Internet.

Pedophiles pose another danger to children on the Internet. Pedophiles "hang out" and even lurk where children play. Today the computer is the playground of the new millenium where pedophiles befriend children, gain their trust, and can lure them from home and molest their prey. Recent newspaper articles report that there are numerous computer bulletin boards set up specifically for the seduction of children. Many parents are unaware that their children are at risk.

Enough Is Enough (EIE) is committed to preventing abuse of children, through education. We believe it is important for the technology industry, the legal community and the public to work together toward that goal.

The Orange County Register, Jan. 19, 1999 issue, in the World Report section, reported; "Abuse at emergency level: The number of sexually abused children has risen to emergency levels, and photos of them are finding their way increasingly onto computer screens, experts said Monday at a U.N. conference in Paris on pedophilia and the Internet."

It is generally acknowledged that the majority of children in this country know far more about computers and the Internet than their parents. Therefore, our children are at risk of either accessing inappropriate material (either intentionally or unintentionally) from the Internet, World Wide Web or e-mail and/or being stalked by a predator in chat rooms and e-mail, without parents or teachers being aware of the situation.

Workable Solutions with Measurable Results: Because of the assault on our children by on-line pedophile activity and the easy availability of dangerous material, Enough Is Enough is committed to taking a leadership role in this cutting-edge issue. We have designed our programs for 2000 around educating school age children, educators, librarians, legislators, law enforcers, and the public – empowering them to *Make the Internet Safe for Children*.

An important part of our communication effort is Enough Is Enough's "One Click " away award winning web site which received well over 1 1/2 million hits in 1999 and is averaging 4000 to 5000 hits per day this year.

Our site was launched in 1995. It was one of the first web sites to cover the issue of Internet Safety. Addressing all aspects of the problems and the solutions, including a dual approach focus on the prevention of child online exploitation as well as victim assistance.

Some of the categories of content include:

- Fun and educational links to sites that are safe for children and families
- Online predators; the dangers and safeguards
- Tips on safeguarding your home and children from pornography on the Net
- Links to filter products and our list of family friendly Internet service providers
- Understanding the truth about pornography and its harms
- Assistance for victims of pornography and sexual violence; referrals, hotlines and more

Extensive marketing and PR efforts have been made to promote the site in combination with our toll free number for those not yet online or Internet savvy.

In addition, Enough Is Enough has established our "CyberPartner" program which encourages our constituents to educate their sphere of influence on Internet Safety. We equip them through e-mail, keeping them informed with current articles, news and EIE resources.

Enough Is Enough believes that this wonderful new technology, the "Internet", is a tool that all of us will be using in the future. But with every new communication medium comes new responsibilities for parents, their children and educators. Our goal is to provide a powerful education program that will benefit all three, so this remarkable technology can thrive, while protecting this country's greatest resource, our children.

Summary: The Board of Directors and staff of Enough Is Enough cherish the freedoms provided by the Constitution of the United States. We also recognize the value of the Internet as an educational resource and a communication tool for students of all ages, businesses and individuals.

The Enough Is Enough staff has worked hard to devise a workable, fair, and constitutionally sound plan for ***Making the Internet Safe for Children and Families.***

Enough Is Enough, P.O. Box 26228, Santa Ana, CA. 92799
714/435-9056 * 714/435-0523 FAX * 1-888-2enough
WWW.enough.org

Preface:

Thank you, Mr. Chairman and Commissioners, for your kind invitation to include my professional insights in this important hearing. Restricting the access of minors to adult web sites is an important issue in our increasingly electronic world. As the CEO of an industry leading Web company, I hope my comments prove to be useful to the Committee's work and ultimate findings. The protection of children from harmful and inappropriate content on the Internet is a goal that we share, and one I am pleased and eager to join with you in accomplishing.

Flying Crocodile, Inc. and the YNOT Network, Inc., properties that together provide information and services to more than 55 million adult Internet visitors each day, share your concerns regarding minors having access to explicit materials on the Internet. I sincerely appreciate having this opportunity to assist you in your efforts to effectively deal with this important issue.

The majority of adult Internet business owners understand the moral and financial implications of the continuing failure of the present system to restrict minors from gaining access to explicit materials. Minors cannot legally purchase such materials via the Internet. Further, the industry has no incentive to serve an underage audience. You can see we are on the same page in our desire to arrive at a solution quickly and effectively. This industry has every reason to be a pro-active and willing participant in the search for a lasting solution in this troubling area.

Unfortunately, some of the top adult websites have an under-18 demographic base that represents as much as 25 percent of their traffic (that is, on 1,000,000 unique visitors per day, they are visited by 250,000 minors per day). This industry condemns this situation and is morally opposed to it. In addition, this is 25 percent of the (very expensive) cost for goods sold that can be eliminated by building a sane, effective solution that will eliminate this pervasive and plaguing problem.

Every day, parents and educators face the problem of minor's access to explicit material. By exploring new and innovative ideas that will grow with the Internet, I am confident that this committee is in the unique position to get this important issue solved.

I am concerned, however, that some of the proposed solutions will create more problems than they solve. Following is a brief discussion of a few of these proposals, along with their associated drawbacks.

Top Level Domains:

One idea passed around for the last few years is the suggestion to create a new dot-porn or dot-XXX domain, then outlaw explicit adult content on all of the dot-com, dot-org, and dot-edu domains. The tracking and enforcing of any new U.S. standard would involve creating a huge and very expensive new bureaucratic and technical infrastructure.

Also, while you can exclude explicit content on dot-com, dot-org, dot-edu and other domains, you will find it VERY difficult to pass enforceable laws regarding the content on sites in Russia (dot-ru), Japan (dot-jp), Canada (dot-ca) and other top-level foreign domains.

Additionally, there would be a MAJOR fight from adult Internet entertainment companies. These companies worry about the ease with which a single adult-content domain pipeline could effectively be crimped by industry critics who could drop traffic to and from these domains as a way to express conservative corporate policy. I think we can all imagine a reasonable scenario of a wealthy individual who objects to adult content buying Teleglobe™ or PSI Net™ just to drop any packets on the dot-XXX domain. Traffic on this single domain could also be unilaterally limited by a state or local governmental agency under the pretense of freeing up bandwidth. The adult companies have real concerns of this kind of private or state censorship, and therefore, are eager to work on more parent- or individual-centric solutions.

I also fear that the imposition of this proposed solution would unfairly discriminate against the adult online industry, which I remind you is a perfectly legal industry. Indeed, our industry is protected by the fundamental law of the land – the United States Constitution. Minor's access to these sites can be accomplished without the unfair, and potentially illegal, imposition of a discriminatory domain.

Hence, I strongly feel that a dot-XXX domain is a very inappropriate and inefficient solution to this issue.

Age Verification Systems:

Age Verification Systems will work to a degree, but only if a new system is put into place (the current systems are not extensive enough). A "boilerplate" of technical and business standards and processes for an AVS system would have to be invented and then backed by the government on a license similar to the one Network Solutions has now. This system might work if all adult Web sites were legally instructed to use the government-regulated system or face enforcement action.

However, proving age over the Internet is a very difficult issue. Credit cards are insufficient as age verification. Many 16-year-olds with bank accounts now have VISA and MasterCard debit cards that work as credit cards online. Another rock solid, impossible-to-circumvent proof of age mechanism would have to be invented. On this, I have no immediate ideas.

Additionally, AVS systems are less desirable because they do not harness the technical power of the Internet in regards to filtering and labeling mechanisms.

Filtering, Labeling and Rating:

I will prepare my full statement on Filtering, Labeling and Rating in time for the July 20-21 hearing, that I hope to attend in person and present written and oral testimony.

I believe that this is a problem which we can work together to solve. It is very important, however, that heavy-handed or ill-considered solutions are not adopted. By embracing creative solutions, we can effectively exclude minors from adult Internet content without violating the fundamental rights of adults, or by crippling a legal industry with Byzantine regulations.

I know that this Commission is committed to developing workable and fair solutions to the challenges posed by an interconnected society. I stand ready to work with you, and I trust that together we can assure a safe online environment for children and adults.

Again, my thanks to this Commission for inviting my input, and I do sincerely look forward to working with you as this process continues.

Kind regards,

Andrew Edmond

ICANN

Letter from Louis Touton to Chairman Donald Telage of the COPA Commission

8 June 2000

June 8, 2000

BY FACSIMILE

Mr. Donald Telage
Chairman
Child Online Protection Act Commission
c/o Kristin Litterst
Dittus Communications
1000 Thomas Jefferson Street, Suite 311
Washington, D.C. 20007

Dear Chairman Telage:

I appreciate the Commission's invitation to provide information concerning the process for introduction of new top-level domains (TLDs) to the domain name system (DNS) of the Internet. Unfortunately, preparation for the upcoming Internet Corporation for Assigned Names and Numbers (ICANN) meeting in Yokohama prevents me from attending these hearings in person. I hope this letter will meet the Commission's needs.

ICANN does not express a position on the advisability of adding a new TLD specifically for adult material. Rather, in this letter it seeks to describe the ongoing process of consideration of the addition of new TLDs generally.

ICANN is the non-profit corporation that was formed in 1998 by the Internet community at the invitation of the U.S. Government's White Paper. ICANN and the U.S. Department of Commerce are engaged in a joint project under which the U.S. Government is, as described in the White Paper, transitioning responsibility for the IP address space allocation, protocol parameter assignment, domain name system management, and root server system management functions to the private sector.

In keeping with the history of the management of the Internet, ICANN uses a bottom-up, consensus-based decision-making process. ICANN is advised by three supporting organizations-the Address Support Organization, the Domain Name Support Organization, and the Protocol Support Organization-comprised of experts and interested participants who examine in-depth the issues facing ICANN and make recommendations to the ICANN Board. ICANN and its Supporting Organizations operate to the greatest extent feasible in open and transparent manner.

For several years, there have been proposals to implement additional TLDs in the DNS. Different types of TLDs have been discussed, ranging from TLDs available for registrations by any person or organization for any use ("unrestricted TLDs") to TLDs intended for registration by particular types of persons or organizations or for particular uses ("restricted TLDs").

In accordance with the bottom-up principle of the White Paper, in May 1999 the ICANN Board referred the issue of TLD expansion to its Domain Name Support Organization (DNSO). On June 25, 1999 the DNSO Names Council created a group, known as Working Group C, to study the issues raised by the introduction of new TLDs. Working Group C deliberated for approximately nine months and in March and April of this year submitted reports to the Names Council. On April 18, 2000, the Names Council adopted a set of recommendations to the ICANN Board.

Those recommendations, which are currently before the ICANN Board, call for the addition of a limited number of new top-level domains (TLDs). The Board is expected to act on these recommendations at its meeting in Yokohama, Japan on July 16, 2000.

Consistent with the recommendations of Working Group C, the Names Council stressed that the introduction of new TLDs should occur in a "measured and responsible manner," as part of an initial test bed designed to enable effective evaluation of the process. The Names Council expressed concern that a proposal to introduce initially as many as ten new TLDs did not enjoy consensus in the Internet community. The proposed limitation on the number of new TLDs to be initially introduced reflects concern about potential dangers to the stability of the Internet if many TLDs are added too quickly. Additionally, because no new generic TLD has been added for many years (since before the emergence of widespread commercial uses of the Internet), lack of experience in the practical implications of adding of new TLDs counsels caution.

Many groups, companies, and organizations have expressed needs and desires for new TLDs, ranging from open TLDs to promote competition with .com, to specialized non-commercial domains to promote advocacy and free-speech values, to a personal domain in which individuals may register their proper names. If the Board proceeds with the addition of new TLDs at its meeting on July 16, it is likely to call for proposals from organizations that wish to sponsor new TLDs and companies that wish to operate TLD registries. ICANN would then evaluate the proposals and select a small number of TLDs from among them according to policies adopted in the Internet community through the ICANN process. The Names Council's recommendations contemplate that, after introduction of this initial round of new TLDs, there will be a review of the experience gained to determine whether additional TLDs should be introduced.

Please let me know if you would like me to provide additional information on the process for introduction of new TLDs.

Sincerely,

Louis Touton
Vice President

Page Updated 10-June-00.

(c) 2000 The Internet Corporation for Assigned Names and Numbers All rights reserved.

COPA Commission

Information and Resources About the Commission on Online Child Protection (COPA)

Hosted by the Congressional Internet Caucus Advisory Committee

Official Hearing Notice

Request for Comments on Filtering, Labeling, and Rating Technologies

ACTION: Request for submission of comments regarding filtering, labeling or rating services in preparation for the July hearing of the Commission on Online Child Protection.

SUMMARY: The Commission on Child Online Protection is directed by Congress to consider methods and technologies to help reduce access by minors to material that is "harmful to minors" (as defined in the Child Online Protection Act ("COPA"). As part of this review, the Commission has scheduled three public hearings to consider these methods and technologies. On July 20-21, 2000, the COPA Commission will hold its second public hearing at the Jepson Alumni Center at the University of Richmond in Richmond, Virginia to consider filtering, labeling, and rating technologies. Today's notice seeks comments on such technologies.

DATES: Comments are requested by Wednesday, July 14, 2000, to permit consideration by the Commissioners in advance of the hearing. However, the record will remain open for receipt of comments until after the last hearing in August 2000.

ADDRESSES: Written comments should be submitted to: Kristin Hogarth Litterst, Dittus Communications Inc., 1000 Thomas Jefferson St., NW #311, Washington, D.C. 20007. If feasible, nineteen copies of the written comments should be submitted. Alternatively, the Commission will accept comments submitted to the following e-mail address: comments@copacommission.org. General submissions should be captioned: "Comments on Second Hearing Subjects."

SUPPLEMENTARY INFORMATION:

Introduction

The Child Online Protection Act, 47 U.S.C. 231 note, ("COPA"), as amended, established a temporary, 19-person Commission to study methods to help reduce access by minors to material that is harmful to minors on the World Wide Web. The COPA Commission is directed to submit a report to Congress, no later than October 21, 2000, on the results of this study, including:

a. a description of the available technologies and methods to reduce minors' access to harmful materials (including filtering, rating, age verification systems, and others),
b. conclusions regarding such technologies and methods,
c. recommendations for legislative or administrative actions to implement the conclusions of the Commission, and
d. a description of the technologies or methods that may meet the requirements for use as affirmative defenses to liability under COPA, 47 U.S.C. § 231, for unlawfully permitting minors to access harmful material.

The COPA Commission will hold 3 public hearings. On June 8-9, 2000, it held a hearing in Washington, D.C. on "one-click-away" resources, age verification systems, and creation of a top-level adult domain. On July 20-21, 2000, it will hold a hearing on filtering, labeling, and rating systems, at the University of Richmond in Richmond, Virginia. On August 3-4, 2000, it will hold a hearing on other PC-based technologies, marketing of pornographic material, and future protective systems, at a location to be determined.

Information solicited by this notice:

In connection with the second public hearing, the COPA Commission requests comments on all issues of fact, law, and policy regarding the operation and implications of filtering, labeling, and rating systems. The following are questions that may be considered at the July 20-21 hearing:

General

1. What information exists regarding parents' awareness and attitudes about Internet filtering?
2. What is the relevance of traditional labeling or rating of movies, music, tv shows and video games to the Internet?
3. What information is available regarding parents' awareness and attitudes about Internet filtering, rating/labeling?

4. What legislation would be most appropriate to promote awareness and effective use of filtering, rating or labeling systems?
5. Should government conduct, sponsor or fund research into improving filtering, labeling and rating systems?
6. Must a filtering, labeling or rating system be international in order to effective?
7. What are the implications of filtering and labeling technologies for privacy, first amendment rights and law enforcement?

Questions specific to filtering

8. How do current filter systems operate, and to what extent do they rely on rating and labeling?
9. What evidence exists regarding the effectiveness of current filter technologies at blocking access to material that is harmful to minors as defined in the COPA statute?
10. To what extent do such systems over-filter, that is, also prevent access to harmless material of interest to minors?
11. How many filter systems are in the marketplace, and to what extent do consumers use them?
12. What prevents more widespread adoption of filtering by parents and public facilities, and what can be done to further their use?

Questions specific to labeling and rating

13. How do current labeling and rating systems operate?
14. What evidence exists regarding the effectiveness of current labeling technologies at restricting access to material that is harmful to minors as defined in the COPA statute?
15. To what extent if any do such systems also have the effect of restricting access to harmless material of interest to minors?
16. How many labeling and rating systems are in the marketplace, and to what extent are web sites labeled or rated?
17. What prevents more widespread adoption of rating/labeling by web sites, and what can be done to further their adoption?

Comments filed with the COPA Commission will be made available to the public.

Public hearing

In an upcoming notice, the COPA Commission will make public the agenda and witness list for the July 20-21 hearing.

[Home] [Final Report] [About this Site] [FAQ] [The Commission] [Press Room]
[Meetings and Hearings] [Research Papers] [Privacy Policy]

webmaster@copacommission.org / Copyright © 2000

COPA Commission

Information and Resources About the
Commission on Online Child Protection (COPA)

Hosted by the Congressional Internet Caucus Advisory Committee

Guidelines for Submitting Public Comments

Since the Commission has completed its work, no more submissions can be accepted. Questions about Commission activities may be addressed to comments@copacommission.org.

[Home] [Final Report] [About this Site] [FAQ] [The Commission] [Press Room]
[Meetings and Hearings] [Research Papers] [Privacy Policy]

webmaster@copacommission.org / Copyright © 2000

COPA Commission

Information and Resources About the
Commission on Online Child Protection (COPA)
Hosted by the Congressional Internet Caucus Advisory Committee

AGENDA AND WITNESS LIST FOR COPA COMMISSION HEARING

July 20-21, Richmond, VA

Thursday, July 20

9:00 a.m. - 9:15 a.m. **Welcome by Chairman Don Telage and Subcommittee Co-Chairs Commissioners George Vradenburg and Donna Rice Hughes**
Purpose: The co-chairs will briefly provide a road map to the matters to be discussed during this hearing, including an identification of the various issues that some believe are raised by filtering, labeling and rating technologies.

9:15 a.m. - 9:30 a.m. **Technical Introduction**
Purpose: To provide a technical overview of the technologies that are the subject of this hearing

- Lorrie Cranor, Senior Technical staff member, AT&T Labs-Research *biography* *testimony*

9:30 a.m. - 10:15 a.m. **Panel One: Client Side Filtering Technologies**
Purpose: Client side filters are tools that reside on the individual's P.C.; often they can be customized to meet the individual user's needs. This panel will describe the technologies deployed in the marketplace, how they operate, their availability and extent of use.

- Gordon Ross, President and CEO, Net Nanny Software International Inc. *biography* *testimony*
- Mark Smith, President, BrowseSafe *biography* *testimony*
- Susan Getgood, Vice President and General Manager, Cyber Patrol *biography* *testimony*
- Richard Schwartz, CEO, Opportunity-America (ClickSafe.com) *biography* *testimony*

10:15 -10:30 a.m. Break

10:30 -11:45 **Panel Two: Server Side Filtering Technologies**
Purpose: Server side filters are tools that operate from a centralized server. This panel will describe the technologies deployed in the marketplace, how they operate, their availability and extent of use.

- Kevin Fink, Chief Technology Officer, N2H2 *biography* *testimony*
- Sunil Paul, Founder and Chairman, Brightmail Inc. *biography* *presentation*
- Stephen Boyles, Library Guardian (Swifteye) *biography* *testimony*
- Michael Stephani, President and CEO, Exotrope *biography* *testimony*
- Ginny Wydler, Director of Standards and Policy, AOL *biography* *testimony*
- Tim Robertson, Founder and CEO, FamilyClick *biography* *testimony*

11:45 a.m. - 12:15 p.m. Comment Period

12:15 p.m. - 1:30 p.m. Break for Lunch

1:30 p.m. - 2:30 p.m. **Panel Three: Rating and Labeling Technologies**
Purpose: Rating and labeling systems rely on some party's analysis of a site, and assignment of a rating or label regarding its content. This panel will describe the technologies deployed in the marketplace, how they operate, and the extent to which sites have been labeled or rated.

- Sheridan Scott, Chief Regulatory Officer/Bell Canada, ICRA *biography* *testimony*
- Joe Field, Co-founder and CTO, Pearl Software/Cyber Snoop *biography* *testimony*
- Ray Soular, Chairman, SafeSurf *biography* *testimony*
- Arthur Pober, President, Entertainment Software Rating Board *biography* *testimony*
- Mike Zimmerman, News Editor, eWeek *biography* *testimony*

2:30 p.m. - 3:30 p.m. **Panel Four: Effectiveness of Filtering, Labeling and Rating Technologies**
Purpose: Exploration of the effectiveness of filtering labeling and rating tools at protecting children, including debates about overbreath and underbreath and concerns about market adoption.

- Herbert Lin, Senior Scientist, The Computer Science and Telecom Board/National Academy of Science *biography* *testimony*
- Christopher Hunter, Annenberg School for Communication *biography* *testimony*
- Zachary Britton, Founder and CEO, Front Porch Communications *biography* *testimony*
- Karen Schneider, Assistant Director of Technology, Shenendehowa Public Library *biography* *testimony*
- David Burt, Founder, Filteringfacts.org *biography* *testimony* *additional testimony*

3:30 p.m. - 3:45 p.m. Break

3:45 p.m. - 4:45 p.m. **Panel Five: Impact of Filtering, Rating, & Labeling on Content Providers**
Purpose: This panel will consider the impact of filtering, labeling and rating on content providers, considering motivations to self-rate, issues of cost and implementation, and the technologies' effects on distribution, reach, and content decisions

- Andrew Edmond, CEO, Flying Crocodile, Inc. *biography* *testimony*
- Scott Fehrenbacher, Vice President, Content Management, CrossWalk.com *biography* *testimony*
- Eric Aledort, Vice President, Corporate Business Development and Governmental Affairs, Disney's GO.com *biography* *testimony*

4:45 p.m. - 5:15 p.m. Comment Period

Friday, July 21

8:30 a.m. - 8:45 a.m. **Welcome by Chairman Don Telage and Subcommittee Co-Chairs Commissioners George Vradenburg and Donna Rice Hughes**

8:45 a.m. - 10:30 p.m. **Panel Six: The Consumer's Perspective**
Purpose: To hear real-life stories about how families, schools and libraries make decisions about use of these technologies, what decisions they make and why, and their surfing experiences thereafter *Consumers:*

- David Biek, Manager, Main Library, Tacoma Public Library *biography* *testimony* *presentation*
- Carolyn Caywood, City of Virginia Beach Public Libraries *biography* *testimony*
- Carolyn Roberson, Norfolk Public Schools, Norfolk, VA *biography* *testimony*
- Carrie Gardner, Milton Hershey School, Hershey, PA *biography* *testimony*
- Detective Mike Sullivan, Naperville, IL police department *biography* *testimony*

Children:

- Elliott from Richmond, Virginia
- Dani from Virginia Beach, Virginia
- Jon from Virginia Beach, Virginia
- Amy from Richmond, Virginia

10:30 a.m. - 10:45 a.m. Break

10:45 a.m. - 12:30 p.m. **Panel Seven: Policy Implications of Filtering, Labeling and Rating**
Purpose: To discuss the collateral implications of these technologies for privacy, law enforcement, and the First Amendment and consider the role of government vis a vis these technologies.

- Larry Lessig, Stanford University School of Law *biography* *testimony*
- Elliot Mincberg, Vice President, General Counsel and Legal Director, People for the American Way Foundation *biography* *testimony*
- Crystal Roberts, Family Research Council *biography* *testimony*

- Colby May, Director, American Center for Law and Justice *biography* *testimony*

12:30 p.m. - 1:00 p.m. Comment and Questions

Hearing adjourned.

[Home] [Final Report] [About this Site] [FAQ] [The Commission] [Press Room]
[Meetings and Hearings] [Research Papers] [Privacy Policy]

webmaster@copacommission.org / Copyright © 2000

Biography
Dr. Lorrie Cranor

Dr. Lorrie Faith Cranor is a Senior Technical Staff Member in the Secure Systems Research Department at AT&T Labs-Research Shannon Laboratory in Florham Park, New Jersey. She is chair of the Platform for Privacy Preferences Project (P3P) Specification Working Group at the World Wide Web Consortium. Her research has focused on a variety of areas where technology and policy issues interact, including online privacy, electronic voting, and spam.

In 1997 Dr. Cranor co-authored a report on tools that support parents' ability to choose online content appropriate for their children. This report was updated a year later and has been widely cited and distributed.

Dr. Cranor received her doctorate degree in Engineering & Policy from Washington University in St. Louis in 1996. As part of her graduate studies she implemented prototype software for one of the first secure and private Internet voting systems.

Dr. Cranor was chair of the Tenth Conference on Computers Freedom and Privacy (CFP2000). She is frequently invited to speak about online privacy, and in 1998 Internet Magazine named her an unsung hero of the Internet for her work on P3P. In the Spring of 2000 she served on the Federal Trade Commission Advisory Committee on Online Access and Security. Her web site can be found at http://www.research.att.com/~lorrie/

Testimony of Dr. Lorrie Faith Cranor before the COPA Commission, 20 July 2000

http://www.research.att.com/~lorrie/

I have been asked to provide a technical overview of the technologies that are the subject of this hearing. I am going to describe to you a taxonomy[1] that I developed with my colleague Paul Resnick, which should provide a useful way for thinking about the different technologies that are available.

Technologies that promote safe and appropriate online experiences for children generally provide mechanisms for 1) identifying or describing content of a particular type, and 2) taking an action based on the type of content. A wide variety of techniques can be used to classify content, and a wide variety of actions can be taken based on the classification. But the common features that I think you will see in most, if not all, the technologies you hear about during this hearing, is that they all employ some classification technique, and some mechanism for taking an action based on that classification.

Classification

Regardless of what actions are taken, mechanisms are needed to identify content of a particular type. If we want to promote or restrict access to a particular kind of content, we must first figure out what that content is. How do we find the educational content to recommend or the inappropriate content to restrict? What criteria do we use to determine what should be recommended or restricted? And who or what actually does the work to identify each kind of content?

Who/how

Classification may be done by a variety of different parties:

- **Third-party experts** may be employed to label content. For example, many filtering companies use teams of information specialists, parents, and teachers to assist in classifying content.
- **Automated tools** may be employed to classify online content. Some of these tools are used to classify content dynamically, as the user requests it. Other tools are used to assist human classifiers in finding suspect sites.
- **Local administrators** such as parents or teachers may personally decide what content should be accessible to children under their supervision. Some tools allow the person who configures the software to provide their own lists of acceptable or unacceptable content by URL or by providing a list of key words or phrases to be searched for automatically.
- **Content providers** may rate or label themselves. For example, many adult content providers post notices on their sites stating that their content is not suitable for

children. In addition, the Platform for Internet Content Selection (PICS) was designed to support self-labeling (in addition to third-party labeling).

- **Surveys or votes** are often used to rate restaurants or movies. This technique has seen some limited use for rating online content.

Classification scheme

Classification schemes may be designed to identify content that is "good for kids" or content that is "bad for kids" or both. The content may be classified on the basis of

- its age suitability;
- specific characteristics or elements of the content, such as what language it is written in or whether it contains nudity or violence;
- or who created the content, such as a distinction between government and non-government sources.

Classification schemes can be designed to be fairly descriptive or very simple. A sophisticated rating system might have 20 variables that must be set, while a simple rating system might have a single "thumbs up" variable. Each system has its benefits. The sophisticated system provides more information, but requires more work to label content and to interpret the labels for each application. The simple rating system is quite easy to use, but conveys less information.

Besides having fewer variables, simple rating systems are also often more subjective. Rating systems may include both descriptive information and subjective opinions about, for example, the appropriateness of content. However, subjective systems can be problematic when users do not know if the bias inherent in the system matches their own. Also, from descriptive information one can always derive a new set of "subjective" opinions. If you are told about the content of a site in terms of violence, language, nudity, sex, and who paid to produce it, one can make a thumbs-up or thumbs-down decision. Given only someone else's thumbs down, however, one cannot recapture the descriptive information. Once opinions replace descriptions, information is lost.[2]

Scope

Internet content is provided through a variety of protocols including HTTP (Web sites), FTP, gopher, chat, telnet, instant messaging, and email. Some products and services focus on one or a small number of these protocols, while others provide more comprehensive solutions, monitoring everything a child does online. In addition, some products and services monitor only incoming communications, while others monitor both incoming and outgoing communications. Tools that monitor outgoing communications can often be configured to prevent children from giving out personal information that could be used to harm them such as their home address or phone number.

Actions

We have found tools that take six types of actions based on content labels or characteristics of online content: *suggest*, *search*, *inform*, *monitor*, *warn*, and *block*.

- **Suggest:** recommend appropriate content for children. A wide variety of Web sites, pamphlets, and books provide lists of child-appropriate content. In addition, some filtering software includes lists of suggested sites for children to explore.
- **Search:** select content that is appropriate for children and matches a query. Internet search engines allow people to enter a query and find all the indexed content that matches that query. Some search engines can be configured to filter the query matches and show the user only those matches that are appropriate for children. Other search mechanisms perform searches over databases that contain only sites deemed appropriate for children
- **Inform:** provide information about the content. Labels, reviews, and other descriptions of content can help parents and other supervisors guide children towards appropriate Internet content. However, in order for this information to be useful, it must be easily accessible. Some tools are designed to provide information about content when a user begins to access that content. This information may be displayed in the form of a graphic or banner on a Web page, or as part of the browser or other software.
- **Warn:** provide information about content and recommend against accessing that content before it is displayed. While mechanisms that inform provide information about content that is being viewed, warning mechanism indicate that content is not recommended, before the content is displayed. These tools can be useful for protecting against children accidentally downloading content that could be upsetting to them. Many adult Web sites include a prominent warning on an introductory page that content on other pages at the site is inappropriate for those under 18 (some include mechanisms for making sure those under 18 cannot access their content, but many rely on the warning as the only deterrent). A tool designed to block content that includes a password override could be used as a warning mechanism as well. Parents could provide a password that their children could use to access content that would otherwise be blocked. Thus children would be warned that the content may not be appropriate, but can proceed to access it anyway if they so desired.
- **Block:** prevent children from accessing content. A wide variety of tools prevent children from accessing inappropriate content. Some filter out specific Web sites that have been classified as inappropriate. Others filter out content that contains words or phrases that have been deemed inappropriate. And others filter out all content unless it appears on a "good for kids list."
- **Monitor:** record for later inspection a list of the content accessed or attempted to be accessed by a user; this may be a complete list or include only the content deemed inappropriate for children. Many filtering tools also include monitoring mechanisms that allow an adult "administrator" to review the log to determine what Web sites the child visited, what email the child sent, or what kinds of chats the child was participating in. Some filtering tools also log all attempts to access content in violation of the administrator's policy.

Mechanisms and Interface

Tools for selecting content can be implemented in a variety of ways, through a number of different technical mechanisms and with a wide variety of user interfaces. Some of the important differentiators between tools include where the tool is located, how it can be updated, and how customizable it is.

Location

The mechanisms that implement the actions described above may be located in a variety of places in a computer system including on the user's personal computer, on a local area network (LAN) or local proxy server, at an Internet Service Provider (ISP), on a remote proxy server, or as part of a search engine or Web site.

- **Personal computer:** Placing mechanisms on personal computers can facilitate their configuration and reconfiguration by parents, teachers, or other administrators. On the other hand, it may also facilitate the reconfiguration of these mechanisms by children, against their parents' wishes and possibly without their parents' knowledge. Some PC-based products have been designed with mechanisms to prevent tampering. Many PC-based products require frequent updates; some can update themselves automatically when the PC is connected to the Internet.
- **LAN or local proxy:** Placing mechanisms on LANs or implementing local proxy servers can be a useful solution in situations involving networked PCs, such as schools and libraries. Centralized configuration is easier for system administrators and harder for individuals to tamper with.
- **Internet Service Provider:** Some ISPs offer services designed especially for children. ISPs may provide filtered Internet access or restrict access to chat rooms, newsgroups, or other types of services.
- **Remote proxy:** Subscribers to remote proxy servers configure their browser software to pass all requests through the proxy server. Some of these services include mechanisms that prevent children from getting around the proxy server.
- **Search engine:** Some search engines return only pointers to content that is appropriate for children.
- **Web site:** A variety of Web sites list content appropriate for children.

Updates

As new content appears, it must be classified if tools that make use of classification information are to stay up to date (this is not an issue for tools that classify content on-the-fly.) Some products and services are continuously updated and include mechanisms for users to easily and quickly take advantages of updates. Others require users to manually download updates.

Customizability

Internet filtering products provide a large range of customization options including: mechanisms for customizing allow and block lists; specifying key words or phrases to trigger actions; specifying categories of content to allow or block; and specifying whether inappropriate content should trigger a block, a warning message, a log entry, or other action. While highly customized products can often address a wide variety of customer needs, unless they are carefully designed they may be quite complicated to configure.

Other Features

A variety of other features are available, including the ability to limit the time of day or the amount of time children are online, provide separate settings and passwords for different children, and prevent children from accessing directories on the computer where their parents store important data. Some blocking tools can block individual words and images on a page, while others block whole pages or even entire sites. Some provide explanations about why they have filtered content, while others block silently. In addition, some tools have child-friendly user interfaces (and parent-friendly configuration procedures).

Discussion

I have outlined the range of tools that support parents' ability to choose online content appropriate for their children. When I first inventoried these tools in 1997, I found about three dozen tools that were available at that time. At last check, GetNetWise.org had found over 120 tools that are currently available. The proliferation of tools in this area has lead to increased innovation and the availability of tools to meet a wide variety of needs. Every community, and indeed every family, has their own standards for what types of content are appropriate for their children. Even within a family, different content may be deemed appropriate for children of different ages. These differences lead to a need for a variety of different tools. The type of computer a family owns, where it is located in the house, and how comfortable the parents are in using the computer may also impact the kinds of tools the family may choose to use. I think it is important that we continue to see a diversity of tools offered in the marketplace. In addition, I would like to see increased transparency from vendors about the criteria they use to classify content so that parents can more easily select the tool that best matches their family's values. This information should be easily obtainable from each vendor's web site as well as on the software packaging.

I hope this brief overview has proven valuable to the members of the Commission, and I would be pleased to answer any questions you might have.

---

[1] Lorrie Faith Cranor, Paul Resnick, and Danielle Gallo. Technology Inventory: A Catalog of Tools that Support Parents' Ability to Choose Online Content Appropriate for their Children. September 1998. http://www.research.att.com/projects/tech4kids/

[2] Lorrie Faith Cranor and Joseph Reagle Jr. Designing a Social Protocol: Lessons Learned from the Platform for Privacy Preferences. In Jeffrey K. MacKie-Mason and David Waterman, eds., *Telephony, the Internet, and the Meda*. Mahwah: Lawrence Erlbaum Associates, 1998. http://www.research.att.com/~lorrie/pubs/dsp/

Gordon Ross
President and CEO
Net Nanny Software International Inc.

Gordon Ross' rich and colorful career spans 30 years as an award-winning Internet filtering pioneer, computer and telecommunications engineer and an internationally sought-after speaker. A grandfather whose personal experience and concerns helped shape his mission to make Net Nanny's products First Amendment friendly, Ross strongly believes in the positive virtues of the Internet. He is a firm believer that education, combined with effective technology solutions, proper funding and training for law enforcement will ensure that the Internet remains an open, safe and helpful resource for the global community.

Since 1993, Mr. Ross has lead the company to a position of solid market and brand leadership, beginning with the industry's first filtering product in January 1995 - Net Nanny. Since then, he has expanded the Company into a leading developer of other security-related products -- PC Nanny, NN Pro and BioPassword -- that perpetuate his mission of providing powerful tools that give users options and flexibility in protecting their digital data.

Mr. Ross is a nationally sought-after speaker and advisor on issues concerning the Internet, privacy, security, child safety and the First Amendment. He sits on the US Congressional Internet Caucus Advisory Board,and in March 1999, testified before Sen. John McCain's Commerce Committee hearing on Internet Pornography. Under his direction, Net Nanny sponsored and sat on the steering committee for GetNetWise, a 1999 Internet industry online education initiative directed at parents. The company sponsored,and served on steering committees for the Internet Online Summit in December 1997 and a follow-up project called America Links Up, a national campaign introduced in September 1998 to educate people about the safe, productive use of the Internet. In November 1998, the Company conducted its own America Links Up event in the Seattle area with AT&T, Microsoft, Edmark and others.

His expertise lead him to speak before international organizations, including the Organization for Economic Cooperation and Development's forum on Internet content and self-regulation in 1998 and the Bertelsmann Foundation's conferences on "Child Safety and the Internet" in 1998 and International Ratings and Filtering in 1999. In April 1998, Ross spoke before the Freedom Forum's annual Technology Conference for Journalism Educators and participated in a panel of technology experts in May 1998 at Harvard University's symposium, "The Internet and Society." He also spoke at "The Internet and Our Children," an event that Net Nanny co-sponsored with Microsoft in May 1998, and featured Senator Patty Murray (D-WA), former Congressman Rick White (R-WA, 1st DST.), the U.S. Customs Child Pornography and Cybersmuggling Unit, the ACLU, and Cyberangels.

Mr. Ross represented the Internet filtering industry at the Federal Trade Commission's hearings on protecting children and privacy in 1996 and 1997,served on panels for the Internet Librarian '97 and '98 conferences in Canada and the United States and participated in a meeting last March with the American Library Association and other filtering companies to discuss the state of the technology. He also offered his expertise to the CyberRisk Conference in 1997, which was sponsored by the National Computer Security Association.

For his exhaustive efforts to ensure that the Internet is a safe, open medium, Ross received the first annual Internet Humanitarian of the Year award in February 1999, from CyberAngels, an online Internet safety organization (a division of the Guardian Angels). He also won the Ethics in Action Award in 1999 for individual ongoing corporate responsibility and was presented the Christian Computing Award in 1997 - all in recognition for his long-standing contribution to further public understanding of the important issues surrounding child safety and data security online.

Prior to Net Nanny Software International Inc., Ross developed expertise in information flow, routing, access control and network management while working as a traffic engineer at BC TEL, the largest GTE operating company in Canada. As the Network Systems Manager, Ross was responsible for maintaining BC TEL's highly complex routing and communications systems,overseeing the development of the company's NICS (Networking Information and Communications System). During his 14-year tenure at BC TEL, Ross also served in Beijing, China, teaching network management to Post and Telecommunication Staff in Beijing.

Mr. Ross graduated from California State Polytechnic University in 1973,holds a Bachelor of Science Degree in Electronics Engineering, and is a registered Professional Engineer. He attended AT&T's Network Management School and has taken numerous management courses from GTE. He also owned and operated a professional 24-track recording studio for 9 years and has training and experience in television service and design.

Testimony of Gordon Ross, President and CEO
Net Nanny Software International, Inc.

COPA Commission Hearing
"Filtering and Labeling"

University of Richmond
Richmond, VA
June 20, 2000

15831 NE 8th, Suite 200, Bellevue, WA 98008
Phone: (425) 688-3008, Fax: (425) 688-3010

Introduction

I appreciate the opportunity to be here today before the COPA Commission to discuss client-side filtering technologies. Few technologies have been given as much attention, generated such controversy and caused so much confusion. This is largely due to conflicting views about how they *actually* work versus how people *think* they work. One thing is certain – according to the Annenburg Public Policy Center, three-quarters of parents in the U.S. are concerned about what their kids are doing online and want to do something about it. There is clearly a need for filtering technology. Why is it that only one-third has chosen to use them?

Some argue that consumers don't think filters are necessary while others argue that consumers don't know enough about online dangers to recognize the need for filters. Still others claim that consumers are paralyzed by mixed messages. And it's no wonder. On one hand, filters are supported as effective alternatives to Internet legislation and, on the other, they are dismissed, as ineffective tools that threaten our right to free speech – at different times these opinions have even come from the same source! Given this discrepancy, it understandable why filters have been slow to gain widespread adoption.

The goals of protecting children online and promoting the unfettered growth of the Internet are both noble, but often they are seen as mutually exclusive. Each side cancels out the other's argument, offering equally compelling evidence to support its point. It's time to focus our energies, which is why I am encouraged that the COPA Commission and others are committed to addressing both concerns. I am pleased to have the opportunity today to help increase understanding and build cooperation among these interested parties.

What is a client-side filter?

A client-side filter, like Net Nanny and others, is a software program that is installed on an individual computer, giving the parent varying degrees of control over how and when Internet content is used. Not all client-side filters work exactly the same way, though there is the tendency to lump them together. Each company has its own business and product models, its own way of building enhancements and maintaining databases. Each company markets its product differently and has a distinct philosophy.

The one thing we do have in common is that we provide tools to control children's online activities. Generally, client-side filters work by comparing content against a database of Internet addresses, and in some cases, a words and phrases list. A filtering program, depending on how its configured, can allow or prevent access, log activity, send warning messages or terminate the Internet connection. Client-side filters can also control the transmission and reception of certain words and phrases, including personal information. Some client-side filters provide activity logs that report sites visited, personal information sent and time spent online – for each member of a household – which can be useful for ensuring that rules are followed.

Many people think that if a filter is installed, it automatically blocks access to content. In many cases, parents choose other options that don't involve blocking at all. A good client-side filter carries out a parent's specific wishes and follows a child's online activities regardless of which ISP, search engine or other Internet program is used. Some client-side filters provide all of the features mentioned above, others offer more or provide less. While a client-side filter requires more involvement, it usually provides more flexibility than other filtering options.

Alternatively, server-side filters, which are offered through Internet Service Providers, control content before it reaches an individual computer, requiring little or no involvement from the parent or caregiver, which many parents prefer. Though less so than client-side filters, server-side filters do offer some measure of choice, particularly by age group and category of content, but because they are built to address the needs of a large group of users, they are unable to match a client-side filter's granular controls. Some parents and kids who access the Internet through a filtered ISP can't always access content they need, and are forced to either turn off the filter or choose another ISP that doesn't make the filtering decision for them. Kids can bypass server-based controls by getting their own ISP accounts or using other tactics that exploit security holes, but client-side filters can also be vulnerable.

It is important to note that one approach is not necessarily better than the other; each has its own strengths and limitations. Parents need to choose what is right for them. In some instances, consumers can benefit from using the solutions together, but it is important to know exactly what is gained or lost by combining the two.

Whichever option a parent chooses, the importance of parental or caregiver responsibility must not be underestimated. Using a filter doesn't mean that parents shouldn't continue parenting, it simply makes their lives a little easier and offers some peace-of-mind, by serving as an electronic extension of their own values system. It is crucial that parents ALWAYS pay attention to what their kids are doing online. They need to make sure that the filtering program is operational and hasn't been bypassed by their young "technical wizard." They also need to consider accessing a filter's logs and a browser's history file to see if their rules or instructions have been violated. By paying attention to their child's behavior and going online themselves to learn what their children are doing, parents and caregivers have the means to step in when necessary.

Client-side filters are often accused of failing to be 100% effective. Those of us, who have been in the industry for several years, understand that it is impossible to please 100% of the people 100% of the time. We do, however, listen closely to our supporters and our detractors so that we can adapt our technology to address their concerns. New tools are emerging that will allow the filtering programs to do a better job of keeping up with the massive growth of Internet content, however, it is impossible to capture every site that may be considered inappropriate for children. Innovation is a constant in the technology industry and filters continue to benefit greatly from constant feedback.

Client-side Filtering and the First Amendment

The notion that client-side filters are incapable of supporting the First Amendment is false. The filtering industry continues to be plagued with First Amendment controversy, because the products have been known to block access to unobjectionable and/or constitutionally protected content, depending on the way they are used. The vast majority of the filtering industry pays lip service to the First Amendment, but fails to provide tools that actually allow individuals and organizations to choose for themselves what content is suitable or not for their children.

Since offering the world's first Internet filter in 1995, Net Nanny has successfully navigated the turbulent waters associated with protecting children online and preserving one of our most cherished rights – the right to free speech. From the beginning, we recognized that while pornographic, violent and other objectionable material would continue to grow; it would never overshadow the overwhelming amount of positive material available to benefit children. Giving parents and caregivers the tools to steer their children toward the positive and away from the negative, without jeopardizing the rights of other Internet users, was never seen as impossible. We saw it as the "best of both worlds."

Net Nanny subscribes to the belief that filtering products must not only protect children online, but also respect the First Amendment. Products like ours demonstrate that it is possible to achieve both of these goals by providing full access to, and control over, the database of Internet addresses and words and phrases. While some members of the filtering industry give users the ability to choose which categories of content to block, this should not be confused with full disclosure.

While it is necessary to build a database and keep it updated, consumers should have the ability to analyze each and every site in the database and allow or disallow access based on their own needs and value systems. Consumers should not be put in a box that forces them to adapt to someone else's idea of what is best for their situation. It is not a corporation's right to arbitrarily decide what is best for people who use filtering programs. We must give consumers the power to determine that for themselves. In a free society choice is key, unless perhaps the content is illegal, such as child pornography.

Some companies choose to view their databases as proprietary and therefore shield them from their customers. Their decision may be based on their business models, because many of them make money charging subscription fees for database updates, or other reasons that support their corporate philosophies. It remains clear that filtering solutions, which fail to provide full disclosure, will always be criticized - so much so that even solutions like Net Nanny, which DOES provide full disclosure, occasionally gets lumped with all of the rest. It just makes sense to give people complete control over a filter's database. To do anything else simply detracts people from seeing the valid need for filters.

It is technically possible to filter sites according to a certain set of standards – they could be legal or they could be personal. The difficult proposition is reaching agreement about what constitutes obscenity and what constitutes content that is "harmful to minors." The technology, itself, is capable of housing just about any sort of content that a person, group or law requires – the trick is properly identifying it.

Filtering criteria and ratings systems

Another important aspect to consider is the criteria used to build a filter's database. What kind of agenda is a filtering company promoting? Who are the people making decisions about which content should be included? When dealing with child safety, we must know on what grounds an individual is considered an expert? No matter what their qualifications, people have agendas and have been known to break the law regardless of their profession or whether they have children. It is for these and many other reasons that consumers, who use filtering programs, must remain vigilant. People directly responsible for protecting children should always make the ultimate content decision.

Ratings systems are also problematic. These systems, which categorize and identify Web sites based on a common set of criteria, sound feasible in theory but are less so in the real world. They raise concerns similar to those associated with building databases. Who is making the rating decision and can this approach address the wide variety of needs and sensibilities that exist within the global Internet community? What are the criteria for rating sites? Do they take into account cultural, and societal norms? What is acceptable in this country is not necessarily going to be accepted in a more conservative or liberal culture. It remains to be seen whether ratings systems will catch on, but the filtering industry should continue to work closely with those who are developing a ratings model and incorporate accepted technical standards to increase consumer options.

Cooperation with Internet Industry

Constant technological changes can and do affect the performance of filters from one day to the next. It is our hope that companies who produce chat, instant messaging systems, search engines, browsers and other Internet technologies will step up their efforts to share important technical information with child safety software vendors. Just as the telecommunications industry depends on common standards and agreements to deliver superior voice and data services, the filtering industry needs cooperation and disclosure from a variety of Internet software vendors to continue to provide effective solutions. In an intensely competitive environment, cooperation often takes a back seat to proprietary goals. When it comes to protecting children online, the industry must make more of an effort to ensure technical compatibility. Communication *can* be enhanced without jeopardizing market advantage. We are encouraged that a few prominent industry leaders recently agreed to increase their cooperation, and we look forward to more companies doing the same.

How can the government help?

Many tools are available to help protect kids online, but most people aren't informed enough to know whether they need a filter or that filters are useful. Technology is often more daunting to parents than to kids. Before parents can even feel comfortable taking an active role in protecting their children online, they need to understand the problems associated with the Internet.

Firsthand experience has taught our company that education is key to protecting children online. It must focus not only on children, but on parents as well. Each month, we team up with law enforcement and other computer security specialists to teach a free eight-hour class called the "Internet and Your Child" to parents, teachers and law enforcement. These people are interested in Internet safety and practical tips for improving children's online experiences. Some of them have computer experience and understand the dangers associated with the Internet, but most do not. The curriculum covers a wide variety of Internet concerns and the major technical methods for managing Internet access. It maintains neutrality by providing objective information and encouraging attendees to make up their own mind about ways to control the Internet. One of the most significant resources we use is GetNetWise – an excellent online resource for information on tools, reporting trouble and accessing positive online content.

The classes have a secondary benefit in that they help to create a lasting community network of concerned people who come from different backgrounds. Through IYC's Web Community on MSN, attendees continue to benefit from additional knowledge sharing and camaraderie among IYC participants across the country. In every sense of the word, this is a grassroots public/private partnership that is supported by the goodwill of a handful of people and companies. While it is making a very positive impact, it needs additional resources to meet the overwhelming demand for Internet training.

The government should make it a priority to encourage the growth of educational programs such as IYC through endorsements and the creation of public-private funding partnerships. It should require that straightforward information on current and proposed laws be posted in a central location that is easily accessible, so people are up-to-date on the legal climate. It should also expand funding for law enforcement to ensure that it has the latest technology and training to fight crime. Over 90% of the police departments in the U.S. have 50 officers or less making it difficult for departments to expend the resources necessary to meet demand. Federal, state and local agencies need to be encouraged to find more efficient ways to work together, and with their counterparts overseas. It is crucial that they learn more successful ways to navigate jurisdictional lines that have been complicated by the Internet. And finally, the government should continue to promote user empowerment technologies that put control into the hands of individuals. They want and need protection that suits their own situation. Free enterprise ensures that these technologies are available and that they will continue to improve.

Summary

It is my hope that people involved in protecting children and the integrity of the Internet will seek to find a middle ground where both goals can be met through accurate product and issue analysis, sharing of constructive ideas and a willingness to look beyond individual agendas to achieve a workable solution. The alternative is more confusion for consumers and the danger that both child safety and our constitutional rights will fall through the cracks. Like most things, client-side filters are not perfect, but they will reach their potential if they are built with constructive input from people who care. Ideally, their potential will be reached when people understand that filtering tools should never replace parenting in the digital age, but rather assist it. With the proper combination of technology, education and policies, we will succeed in protecting children online and preserving the integrity and openness of the Internet.

Thank you.

Mark W. Smith
President, CEO and Director
BrowseSafe.com

Mark W. Smith, President, CEO, and Director, has overseen the development of nearly a dozen sophisticated computer software programs currently serving the electronic publishing marketplace. His expertise is in development and management of database programs, office management programs and Educational/Entertainment products. In 1986, Mr. Smith began work as an independent computer and management consultant for businesses throughout the Midwest. From 1992 to May 1999, he served as Director of Electronic Publishing for an Indianapolis-base publisher of books and electronic media. Mr. Smith graduated from Anderson University in 1980 with degrees in Business Management and Marketing.

A Paradigm Shift In Managing the Internet Experience

Maintaining First Amendment Rights While Keeping Our Children Safe

Mark Smith
CEO of PlanetGood Technologies, Inc.
7202 East 87th ST.
Suite 109
Indianapolis, IN 46256

A Paradigm Shift in Managing the Internet Experience

It is a pleasure to be here. Today, I am going to address the issues of an Internet experience – this includes freedom, choice and safety for all children. The Internet is a vehicle for the expression of free speech by a wide and diverse group of World Wide Web content publishers and consumers of that information. The Internet by its own merit is a playground of expression, of ideas, of information, of entertainment and of assorted content. The expanse of diversity and worldwide creativity makes the Internet unique to anything throughout the experience of human kind. Everyone is coming to understand and embrace the good that it represents!

The question at hand is how do we provide freedom and choice of the experience for families in an environment of safety? Most products focus on either a client side technology (cst) base or a server side technology (sst) base. CST means that all the technology is located on the computer's drive (which makes it vulnerable to hacking), and SST means that all the technology is located on a corporation's server (which means the user has limited choice in what is viewed on the web). What would happen if the benefits of each could be brought together to provide the user a new more flexible and powerful way of surfing the web? What if the most up to date search technologies filtered out pornography links and offensive search terms? What if every sub-domain of every site had been categorized and classified by its content? What if the categories were descriptive enough for each site through dozens of unique characteristics? Wouldn't you agree that everyone could benefit from that combination of technology? Of course, they would.

Now let's walk across the street and view this from the parent's perspective. What if parents were able to determine what the child sees? What would it be like if email, instant messaging, and other computer tools could also be controlled? What if the child could not get around the programming no matter how good a hacker he/she is? What if a product, by its very design, is an all encompassing tool that can be used to manage content for every family member regardless of their value system, moral beliefs, age, ethnicity, cultural background or ethical bent - because the very nature of the product is designed to allow the parent or the administrator to enable selectable web content criteria. Shouldn't parents have the right to surf the web freely with no restrictions yet have the peace of mind to know their child can surf the Web safely? Of course, they should. So, why aren't we looking for the technology and resources to combine these benefits instead of trying to position parents to settle for either an sst product or a cst product that will not satisfy everone?

What would it be like if any Internet Service Provider a family chooses could be used with this technology? What if it didn't matter if the ISP had the capability to filter content? Wouldn't that give the parents even more free choices of what they want?

Why are we not trying to put the responsibility of a child's safety in the parent's hands? Why are we not trying to invoke life, liberty, and the pursuit of *happiness in the decisions of parents? Let's be very careful to not expose our* children to offensive or adult material, but let us be equally careful not to undermine the role of a parent to choose what is appropriate and what is inappropriate for his/her children. We should be striving to empower parents instead of imposing regulations that will impact the values and autonomy of the family!

Now that some of the Internet issues have been addressed, let's focus on legal issues that the Commission posed in its letter of invitation.

First of all, PlanetGood believes the approach of a combined sst/cst process is unique and has next to no downfalls. This technology would be the best solution to provide for Internet safety.

PlanetGood's pricing structure does not pose a financial barrier to most parents with computers in their home. It is only pennies per day.

At its core, PlanetGood is an EMPOWERMENT tool for families as well as schools and libraries. The decisions about what is and is not appropriate for family members should be made in the home. Our approach allows the user to experience all the good and none of the bad, **as defined by the parent or administrator!**

Those who publish content on servers that they do not configure or control can use the PlanetGood technology. Nothing is ever totally or permanently inaccessible while using PlanetGood. A parent always has the choice to override or to preview the site with his/her password. The PlanetGood user is alerted onscreen to the fact that there is material online that has been rendered inaccessible and the reason it is inaccessible. Our unique technology can be set to limit access to images as well as to text, audio, video, and chat. It operates in a predictable and transparent way. It works in a seamless way on your computer, so you don't even know it's there - it's just working in the background. Once it's installed The product installs easily and can be customized for each family member. Most of the work is done on the server side. PlanetGood has been developed to also deal with active messages such as incoming e-mail, instant messaging and online chat rooms as well as web surfing.

PlanetGood technology has no side effects on the development of Internet standards or on the conduct of other activities on the net except to encourage rich and safe Internet experiences for families as they see fit. Planet Good does not raise first amendment issues because of the way our product has been developed and used by the customer in a localized manner. PlanetGood is all about freedom and choice. The product simply allows parents to exercise their own judgment on appropriate Internet content for their family. It can be tailored for each and every household, school or library. We believe this to be true whether the product was in widespread use or use was mandated. Although, we believe that it is against our personal freedoms for the federal government to mandate any particular technology or method, the PlanetGood approach is a sound solution for families to keep their children safe.

A Paradigm Shift in Managing the Internet Experience

PlanetGood could be perceived as a less restrictive measure than COPA and therefore, could be viewed as undermining the constitutional validity of laws imposing more restrictive legal obligations. PlanetGood is a new paradigm in what has traditionally been called the filter space. PlanetGood is not really a filter because people have the complete freedom and choice to choose what content they want. Parents can say, "I don't want any filtration. But for my kids, I would really like to restrict some of their activities online when I am not able to supervise them." It's just like a person can restrict certain movie channels and TV shows via a V-chip. It's really no different. What is really unique about PlanetGood is that web content can be selected for each child based on their age and the value system intrinsic to each family or community throughout the country.

PlanetGood would impact legitimate law enforcement activities positively. Currently, my staff is pursuing various activities with law enforcement and crime prevention organizations that is practical and within the parameters of sound judgment.

The people of PlanetGood Technologies set out to provide an on on-line experience that would protect our freedom and provide safety by offering choice for everyone using our service. PlanetGood has the technology we talked about in this testimony. Our product, PlanetGood, does not pretend to be a filter – it is a web content management tool. Parents, local communities, school board members or librarians establish predetermined content for the children they oversee. PlanetGood empowers them with carefully designed selectable criteria to assist decision makers as to what content is appropriate for the children they oversee. A dedicated, well-trained, responsive staff supports the server side technology that enables freedom and choice for management of specific web content. However, it is our highly trained human review team that ensures the integrity of the PlanetGood web content information service. This is true and consistent with our mission statement to be the Internet experience provider offering a unique combination of freedom, choice and web content management for all users accessing our system. We as a company do not set the standard or content for the flow of web information. Simply put, PlanetGood is the tool by which information is disseminated to the end user for an experience that provides all of the Good and none of the Bad.

As a closing thought, this COPA commission has a significant purpose. It needs to act more like the judicial branch than the legislative branch. This commission must weigh the products that filter, rate, etc., and you need to help the Congress/Senate weigh the rights of the family and ultimately that the greater good of the country is ensured. By a legislature's very nature, they want to protect through laws that keep bad things from occurring. The challenge, it seems, lies in the thought of conflicting with the 1st amendment. As you know, whatever this panel decides will ultimately be judged. Judged by legislatures for content, judged by the courts for Constitutionality, and judged by our fellow Americans for the right to be responsible parents. Let us weigh carefully and choose wisely to ensure these inalienable rights that our forefathers entrusted to us and many of them died for. Let us go forward ensuring these rights to our children. Let us stand as one body, one Nation that will secure our freedoms and truly protect our children.

SUSAN GETGOOD
Vice President and General Manager of Cyber Patrol.

Susan Getgood assumed her current position in January 1999, after serving one year as Director of Corporate Communications for The Learning Company. Previously, she was Director of Marketing at Microsystems Software, the Internet software company that developed the original Cyber Patrol Internet filtering product and was one of the first two companies in the world to offer an Internet filter. Microsystems Software was acquired by The Learning Company in 1997.

Ms. Getgood has been involved in Internet children's issues for more than four years. During her tenure, Microsystems Software in 1996 supported the coalition that successfully challenged the Communications Decency Act. Her combination of technical expertise and understanding of issues facing schools and families has made her a valuble resource for both federal and state policy makers. Ms. Getgood has testified twice before the Federal Trade Commission on Internet safety and online privacy, and participated in a panel at the White House Summit on Children's Safety that discussed Internet filtering issues. Cyber Patrol was among the sponsors of the 1997 Internet/Online Summit: Focus on Children. Most recently, Ms. Getgood has been working on issues surrounding positive digital content for children and the development of quality educational content for home and
school.

Ms. Getgood has a Bachelor of Arts degree from Wesleyan University and an MBA from Rivier College.

Comments Before Children's Online Protection Commission
Susan Getgood, Vice President and General Manager
Cyber Patrol

Cyber Patrol was one of the first Internet filtering tools introduced into the marketplace, which provides us with a unique perspective that I'd like to share with you this morning. I hope to make three important points that demonstrate that Internet filtering is widely used, very effective and improving in response to demand from an increasingly sophisticated audience of parents and educators.

First, Internet filtering software is very widely used despite some misconceptions that families don't understand that technology is available to help manage their children's time online.

- More than 9 million families are using Cyber Patrol directly through us or through online services like America Online.
- There are more than 17,000 installations of Cyber Patrol in schools or school districts across the country.
- We have seen roughly 50 percent year-over-year growth in online purchases of Cyber Patrol through our Web site.
- And, this growth is just Cyber Patrol alone and just in the United States.
- SurfWatch is installed in over 8 million homes across the nation and a growing list of online services including ISPs (like excite @ home), ASPs, Internet Appliances (like WebTV and Netpliance's iOpener), and Search Engines (like Alta Vista and Google)

Second, Internet filtering software works. Filtering software today is very sophisticated, effective and easy-to-use.

- Filtering software products that have been in the market for a few years are mature products that strike the balance between sophistication and ease of use.
- Cyber Patrol allows the filter to be tailored to the maturity of the individual child.
- Critics accuse Internet filters of either being overbroad and filtering too much or being too narrow and not filtering enough. Some critics confuse censorship, which is imposed by the government, with technology that a family or school can choose to use and then set to implement an individual policy.
- But the point is to empower parents and schools to make the choices that are right for their individual kids or students. And that's what filtering software does very very well.
- This is our role and it is a role that the U.S. Supreme Court believed was a less intrusive way than government censorship for safeguarding kids and protecting the First Amendment.

Finally, Internet filtering software meets the needs of increasingly Net savvy customers.

- When we began selling software five years ago, we were often marketing to parents and schools that were fearful of a new and unknown medium portrayed by the media as a cesspool of pornography.
- Today, five years later, a lot has changed. Families now shop online, book vacations and check their stocks, schools set up Web sites, have Net access in every classroom and are filled with kids who can surf as soon as they can read.
- People are no longer fearful, they are knowledgeable and understand how to use technology.
- I'm not just the head of Cyber Patrol, I'm also a new mother and I can tell you for sure that parents learn what they need to learn to take care of their

kids – from heating a baby bottle to safeguarding their children in cyberspace.

- Parents and educators are using filtering software without the government telling them to and I believe they will continue to do so.

To underscore this point, we recently surveyed schools using Cyber Patrol and found that about 80 percent had adopted acceptable use policies before they installed filtering software. These schools found that combining technology with clearly stated use policy was most effective in protecting kids. It's common sense.

Cyber Patrol has recently become part of SurfControl Software, a maker of filtering products for the corporate market. This new marriage presents new opportunities for educating the public. For example, we hope to develop programs for educating corporate employees who have children about technologies for protecting their children from inappropriate content. We believe the now mature Internet filtering industry should work together to educate the public. And, we call on the government to help create a public-private partnership geared toward better informing families, schools and other computer users about the best technologies available today.

I thank you for this opportunity to speak with you, appreciate your listening and am happy to answer any questions you may have now or in the future.

Richard J. Schwartz, Co-Founder of ClickSafe.com, was formerly Senior Advisor to New York City Mayor Rudolph W. Giuliani. At City Hall, Mr. Schwartz oversaw New York City's privatization and government reorganization initiatives, including the creation of the City's Department of Information, Telecommunications and Technology (DoITT). He also directed the City's $4.2 billion capital construction program and advised the Mayor on education and housing policy. Mr. Schwartz was also responsible for implementing the City's landmark welfare-to-work program, which has resulted in a reduction of over 500,000 recipients during the program's lifetime.

Mr. Schwartz currently also serves as President and CEO of Opportunity America, a welfare-to-work and workforce development consulting company.

He holds a BA from Columbia University and a Master's in Public Policy from New York University. He has also served as a Senior Fellow at the Manhattan Institute.

Outline for Testimony
Presented by
Richard Schwartz
Co-Founder
ClickSafe.com

Providing a safe and rewarding Web-browsing experience is of great concern to parents, teachers, government leaders and businesses. Education campaigns and public commissions – such as the Copa Commission – are helping to raise awareness and stimulate emerging technologies to address the issue of inappropriate content on the Internet.

ClickSafe was developed by some of the nation's most accomplished technology experts to solve this problem with what, we believe, is the Internet's most accurate and advanced pornographic filtering technology

Limits of Currently Available Filtering Programs:

- Virtually all filtering programs must maintain blacklists of inappropriate Web sites. These lists must be updated regularly.
- The accuracy and performance of these filtering programs can be limited by the resources available to search the World Wide Web for pornographic sites.
- Many pornographic sites make this process more difficult when they hide their real content from filtering programs.

ClickSafe's Breakthrough Technology

- **ClickSafe**'s uses state-of-the-art, content-based filtering software that combines cutting-edge graphic, word and phrase-recognition technology to achieve extraordinarily high rates of accuracy in filtering pornographic content.
- **ClickSafe** operates in real time by filtering the Internet instantaneously through its combined image, word and phrase-recognition technologies. This prevents the possibility of "pornographic hijacking" or inadvertent access to newly-created or renamed pornographic sites.
- **ClickSafe** can precisely distinguish between appropriate and inappropriate sites (i.e. it has both remarkably low underblocking and overblocking rates).
- **ClickSafe** can be easily customized to block or accept any sites, as desired by the system administrator.
- The **ClickSafe** technology resides within the computer/server and requires no updates of blacklists or interactions with a central host service.
- **ClickSafe** offers what may be the most effective and most economical universal solution for filtering pornographic content from the Internet.

Kevin Fink
Chief Technical Officer
N2H2

Kevin helped launch N2H2 in 1995 and developed the Company's pioneering filtering proxy-server. He sets N2H2's strategic technological direction, oversees all technical staff, and drives product development. Mr. Fink has more than 14 years experience with a wide variety of computer systems and programming languages. Prior to joining N2H2, Kevin was MIS director for Virtual Broadcast Network, one of the first web hosting companies in the Pacific Northwest. Mr. Fink received his B.S. degree in Engineering from Harvey Mudd College, and his M.S. degree in Electrical Engineering from the University of Washington, where he is currently on leave from a Ph.D program.

Written Testimony of Kevin Fink, Chief Technology Officer, N2H2, Inc.
Commission on Child Online Protection (COPA)

July 20, 2000

I. Introduction

My name is Kevin Fink and I am the co-founder and chief technology officer of N2H2, Inc, a publicly-traded company based in Seattle, Washington. I would like to thank the COPA Commission for the opportunity to tell you more about N2H2 and our approach to Internet filtering.

Specifically, I will focus on:

1) An Overview of N2H2's Market Presence.
2) N2H2's Principles of Internet Content Management.
3) How Our Technology Supports Our Principles
4) Closing Thoughts on Future Advances in the Filtering Industry.

II. An Overview of N2H2's Market Presence

N2H2 is a leading Internet infrastructure company specializing in filtering, Internet management and content delivery services for schools, home and work. While expanding now into the corporate and home markets, the company has built its reputation on its presence in the K-12 education market. We combine advanced Internet technology and human review to make the Web more meaningful to 12 million student users over an established network of more than 1,500 Internet appliances in the U.S., Canada, Australia, U.K., Japan, Germany, Mexico, Chile, Bermuda, India and China.

N2H2 is trusted by:

- Over four times as many schools as the next closest competitor (Quality Education Data, 5/99);
- Over 58 percent of school districts with server-based Internet filtering;
- Over 15,000 schools and libraries;
- Statewide networks in Ohio, Tennessee, Maine, Iowa, Idaho, Arkansas and Wisconsin, as well as major school systems in Los Angeles, Baltimore, Boston, Brooklyn, Bronx, Long Island, Dallas, Calgary, Seattle, Stockton, Tampa and many more;
- Over 75 percent of Australian schools.

III. N2H2's Principles of Internet Content Management

At its core, N2H2 is a technology company that answers a demand in the marketplace. We have no ideological axe to grind. We simply try to develop the best possible technology solutions by listening to our customers' needs. In building and improving our services, three market-driven principles guide the process:

1) We focus on choice, customization and control.

This is paramount. We do not keep a "blacklist" of sites and force that list on customers. We allow customers to choose their Internet content. While the Internet explosion is creating exciting new opportunities for education, entertainment and commerce, issues still abound:

- Parents, teachers and employers want the power to choose what Internet content is safe, productive, relevant and/or bandwidth friendly.

- What is considered acceptable or productive Internet content for children and employees varies with every geography, organization, culture and household.
- Privacy issues abound that limit the public's confidence to freely communicate or conduct business over the Internet.

2) ***We strive to deliver the most sophisticated and accurate database.***

We use artificial intelligence and proactive human review to continually add to and maintain our multi-million-entryURL database.

3) ***We offer a complete, comprehensive service solution***.

We strive for a "turn-key" solution. Our goal is to become transparent to the user and hassle-free for the system administrator.

IV. How Our Technology Supports Our Principles

1. We focus on choice, customization and control.

Our content management solutions are based upon choices that empower customers with the ability to create the customized Internet they want.

Feature #1: We separate URLs into categories and allow our customers to choose which categories are appropriate for their network.

To deliver the Web that our customers want, we need to offer flexibility in what is blocked. We provide them with an extensive database of URLs that have been marked as belonging to one or more of over 30 content categories (e.g., pornography, sites that promote hate speech, job search sites). Customers may choose to enable or disable content from each of these categories. It's up to the customer to make that decision, although we will provide advice and examples based on our extensive experience with Internet filtering. We have worked with customers over the past five years to build more than 200 customized configurations.

Communities (i.e. schools) define themselves by the things they allow and disallow. N2H2's filtering strategy supports this time-honored process of community self-definition. Initially, we protect our children from items we don't allow and as they grow up and become mature participants in the community, children take increasingly greater responsibility for defining the community. This shift is reflected in the evolution of a filtering system's major role from safety to productivity as students move from kindergarten through the 12th grade.

Feature #2: We offer "exception" categories.

Customers have the opportunity to customize their Internet experience based on content context. For example, copies of The Starr Report, include the "History" exception to sex categories. A school that wanted to block access to most sex sites, but allow access to those of historical significance, including the Starr Report, has the ability to do that. Another often-used exception category is "Text-Only", which many public libraries use to tailor their Internet access policies to match their policies on access to literature. The "Text-Only" category allows them to block sites with pornographic imagery but allow textual erotica. Other exception categories include "Education", "For Kids", "Medical", and "Moderated".

Feature #3: We allow local overrides.

Customers have the ability to add URLs to or delete URLs from their server's database. It only affects that particular customer's database. For example, if a particular school wanted to allow access to a site giving graphic detail on the Holocaust but wanted to continue to block other sites containing graphic imagery, they could add that particular site to their override database.

2. ***We strive to deliver the most sophisticated and accurate database.***

N2H2's content review process has created the world's largest proprietary Internet filtering database through artificial intelligence and human review.

Feature #1: Automated agents continually seek out candidate sites.

These agents use artificial intelligence to identify and prioritize sites that appear to be relevant to one or more of the categories that we track. They run continuously on a distributed network of over 70 servers, pulling data directly off of the World Wide Web, as well as from Usenet postings, electronic mail, Inktomi's URL database, domain name registration databases, and many other sources.

Feature #2: We use human review to categorize the candidate sites.

Artificial intelligence alone is insufficient to accurately categorize websites. Our Website Analysis Team consists of over 100 people who receive extensive training. They review the content that has been identified by the automated agents and assign categories to each website or portion of a website. They divide each site into sufficiently granular portions to guarantee that each individual page is assigned the correct category or categories.

Feature #3: We leverage our vast feedback loop.

All of the more than 12 million Internet users on our filtering system have the ability to notify us of potentially uncategorized or miscategorized content. If any user locates a web page that they feel should or should not be accessible, they can easily send that URL to the N2H2 Website Analysis Team for review. N2H2 has made this feature easy to access by literally millions of users with a single click from the Block Page or Resource Bar™. This has the effect of expanding our effective review staff from hundreds to potentially millions of people, all working together to build an accurate map of the Internet's content.

3. ***We offer a complete, comprehensive service solution***.

N2H2's Internet Filtering Solution is delivered via a carrier-quality, interoperable, open-architecture system.

Feature #1: We provide automatic nightly updates.

Each night, we update the URL database on each of the more than 1500 servers in our network. Although most of these servers are located on our customers' premises, our systems update them automatically. This keeps the database current without requiring anything of our customers.

Feature #2: We continually monitor and maintain our network of filtering servers.

N2H2's support staff uses a sophisticated system to continually monitor and maintain our network of servers. Each server is continuously monitored for availability and proper performance, and support staff are notified immediately of any issues. In addition, each server is automatically maintained via both internal and remote systems.

Feature #3: N2H2 expert technical support is available 24 hours a day, seven days a week.

In addition to continually monitoring our network of servers, N2H2 support staff are available 24 hours a day, seven days a week to help all of our customers. Because of their extensive networking experience, they are often able to quickly diagnose and provide fixes for customer issues that turn out to be peripheral to our servers. Although not part of our contractual obligations, we feel that our customers are our partners in providing safe, relevant, and productive Internet access, and helping them towards this end is part and parcel of our service.

V. Closing Thoughts on Future Advances in the Filtering Industry

Internet filtering has progressed significantly since its introduction in the early days of the World Wide Web. The first filtering was implemented entirely on client computers, which limited the sophistication of the filtering and the security of the solution. The next wave of products moved to a server-based approach, which offered significantly more sophisticated, and thus accurate, filtering and an extremely secure solution. By centralizing control, however, some individual control was lost.

The next wave of filtering solutions, which are just coming on the market today, will diverge into two paths, depending on the network's requirements. Solutions geared towards ISPs, libraries, and other networks used by large numbers of individuals with specific access needs will use a hybrid approach which will offer the power and security of server-based filtering along with the customizability of client software.

Solutions geared towards corporations, government agencies, schools, and other networks used by groups of users will continue to use a server-based approach, and will become more integrated into overall network architectures. They will work closely with routers, switches, firewalls, and other network hardware components. They will also become integrated with network management systems, so that network policy will be managed at a single point.

In both cases, filtering systems will continue to rely more and more heavily on hybrid approaches, leveraging the intelligence and perception of human reviewers with the speed and tirelessness of computers. These solutions will use artificial intelligence for the tasks which humans aren't well suited to, like individually reviewing every product in an e-commerce database, and human intelligence for tasks which computers aren't well suited to, like differentiating between pictures of the Mona Lisa and pictures of "Mona's Mountains".

URL databases will also continue to become larger, more targeted, and more accurate. When N2H2 began assembling our URL database in 1995, we had two categories: "naughty" and "nice", which were used for all of our customers, whether they were kindergarten classes or 12t^{h-}grade libraries. We added additional lists to accommodate different types of users, then moved to a category-based approach where our customers could build exactly the lists they needed. We continually add categories as our customers indicate the need for additional precision, as well as adding additional customization features such as local override databases and per-user category selection.

In general, filtering systems will become easier to manage and more accurate in their implementation of network policies. They will continue to evolve to keep pace with the evolution of the content they seek to categorize and the access they seek to control. They will also extend beyond "blocking" to offer more direction and help to users who are trying to find particular pieces of content.

Now and in the future, these systems will help to encourage safe, knowledgeable, confident, and productive use of the World Wide Web. N2H2 is working hard to ensure that we remain focussed on satisfying our customer's needs, staying on the forefront of technology and service to allow them to take full advantage of all the Internet has to offer.

Thank you for your time.

Sunil Paul, Founder and Chairman
Brightmail.com

Sunil Paul was inspired to develop a better solution to the spam problem because his personal email accounts were overrun by spam. In October 1997, he founded Brightmail, Inc., a company dedicated to giving users control of their email and enhancing the capabilities of email for the Internet.

Prior to starting Brightmail, Sunil created FreeLoader, Inc., the first company to offer a Web-based push service. In 1996, Freeloader was acquired by Individual, Inc. for $38 million, making it the best and second-best performing investments in the VC portfolios of Euclid and Softbank, respectively.

Before launching FreeLoader, Sunil was with America Online (AOL) as that company's first Internet Product Manager, successfully creating most of AOL's early Internet capabilities. Before AOL, Sunil was a policy analyst at the U.S. Congress Office of Technology Assessment, where he specialized in information technology and telecommunications, including the then-emerging Internet. Prior to that, Sunil spent three years working on NASA's Space Station Information System. He has a B.E. in electrical engineering from Vanderbilt University.

Email Content Control Sunil Paul, Chairman, Brightmail, Inc. Background information for COPA Commission Hearing July 20, 2000

7/20/00

Click here to start

Table of Contents

Author: Jeff Magill

Email Content Control Sunil Paul, Chairman, Brightmail, Inc. Background information for COPA Commission Hearing July 20, 2000

91% of users get spammed at least once/week

Spam and Length of Time with ISP

Spam increase with length of service

Only about 11% of spam has adult content...

...but, consumers perceive 25% of their spam as adult.

Consumers take offense at spam

Complaints about spam only the tip of the iceberg

ISPs Associated with Spammers

ISPs are Looked Upon as Principal Spam Regulator

ISPs don't block spam very effectively

Spam is very costly for ISPs

Stephen Boyles
Senior Technologist
Swifteye, Inc
Greensboro, NC
(336) 378-3725 x2121

Technology Bio:

Stephen Boyles was hired by Image Technology in 1992 to direct the development, implementation and methods used in the realm of commercial Digital Photography. While at ITI, Boyles worked with manufactures such as Sony Electronics, Fuji Photo, Scitex-Leaf Systems and The Eastman Kodak Company to understand both the methods and system requirements that today is used to provide commercial quality imaging and photography without the use of traditional "silver based" means. Boyles also designed the two largest fully digital studios in North America; Salem, MA for Rich's Department Stores and Toronto, Canada for Canadian Tire Corporation.

With the acquisition of a portion of Image Technology by MCI Communications, Boyles became the Director of Digital Imaging for MCI Communications, Inc. Among the normal duties of commercial digital imaging, Boyles specified and developed the hardware necessary to perform digital imaging tasks that were employed in the campusMCI student ID card program. Boyles also investigated and became one of the proponents of SmartCard Technology within MCI working with both IC SmartCards and Contactless Proximity cards and their functions for both physical and virtual security. Boyles won MCI's highest employee award The President Circle in 1995.

Since 1996, Boyles has been basically involved in two distinct technology efforts, the creation of the Digital Key Color Exchange Compositing software, patents applied for October 1997 and the LibraryGuardian Software using SmartCard technology, patents applied for December 1999. Boyles is listed as titled inventor on both technologies.

With LibraryGuardian, Boyles has been very active in not only understanding the 1st Amendment issues surrounding the usage of the Internet in public arenas but has helped to develop a system that is has been embraced by both sides of this powerful issue.

Boyles currently is the Senior Technologist for Swifteye, Inc and serves as Vice President of Product Concepts for the LibraryGuardian division.

#####

Prepared testimony of
Stephen Boyles
Senior Technologist
Titled Inventor –LibraryGuardian
Swifteye, Inc.
120 West Smith Street
Greensboro, NC 27360
(336) 378-7825 x2121

Technology that Empowers Parents

On behalf of LibraryGuardian and the entire staff of developers that have dedicated thousands of hours to the creation of new and unique technologies for enhanced Internet services, it is a profound pleasure to present this testimony to the COPA Commissioners today.

I can vividly remember the President on June 26, 1996 as he closed his press conference on the Supreme Courts' decision to rule certain portions of the Communications Decency Act as unconstitutional "...we must give parents and teachers the tools they need to make the Internet safe for children."

What needed to be accomplished was an Internet server-based solution that provided libraries and schools with the ability to provide unrestricted access to the Internet while in the same environment, also empower parents with the ability to request Internet access for their children in a manner that reflected their own unique values.

Problem #1: Access Management.

Our development team developed a product called "GuardiaNet", a first of it's kind Internet access management software program that allowed a parent to give different access rights to each of their children independently on the same computer. We had extensive experience with SmartCard technology and realized that the integration these two emerging technologies (server-based solutions integrated with SmartCard authentication), we indeed had the beginnings of the technological tools that could make a difference to schools, libraries and of course parents.

We initially built the prototype server-based products around our GuardiaNet technology and selectively showed the SmartCard solution to librarians in 1997. By December 1999, we had completely reinvented the technology and applied for multiple patents for the LibraryGuardian toolbox software.

The evolution of GuardiaNet to LibraryGuardian was significantly influenced by research of community needs and listening to literally hundreds of professional librarians from just about every walk of life.

By observing the "pitfalls" of certain Internet solutions and listening to what we learned from librarians and parents, we realized that a "one size fits all" approach could not a viable solution. We looked at the problem on a more global scale and decided for a solution to be effective, the rules and terms of engagement would have to be very different from community to community. In other words, we needed to provide a custom community based access solutions for every installation.

So in essence, we believed that the answer was right in the President's 1996 statement. We must give the "tools" that allow communities and parents to work hand in hand.

LibraryGuardian is a "toolbox" approach to Internet access management. As a matter of fact, we have not nor will we anytime soon, build or develop technology that is used as a "control list" of Internet content. Rather, we built a toolbox that allows any control list, filtering agent, white or black list to be included and selected by the user. Virtually speaking, any technology listed on "getnetwise.org" could be included for parental choice within the LibraryGuardian toolkit. Currently LibraryGuardian uses Secure Computing Corporation's SmartFilter as the control list default, as well as Awesome Library and KidsClick! white lists for a safe harbor offering. All of these are managed, maintained and continually updated as a part of the service provided by LibraryGuardian.

SmartFilter was selected due to the way it categorize the Internet into 27 definable groups. We found their criteria to be remarkably similar to the way a librarian catalogues physical collections. Not selecting what is "good and bad", but simply placing web pages into categories based around published criteria. This is not completely perfect, but an easy to understand starting point. On top of this, we overlay the administration tools that give the library or school the instant ability to override elements of the SmartFilter control list to best fit the standards of each local community without defeating the core technology.

Thus, the local library or school can have the toolkit that allows it to offer many different access levels based upon their own local standards. LibraryGuardian can be installed in a public facility with one of the access levels "unrestricted" or completely "unfiltered" access, while other levels can be created locally to provide safety to small children, with several levels available in between.

Other locally defined access levels can be created for the community as needed. In other words, a library can select only one filter level that is intended to block access to pornographic web sites or the library could select as many access levels they feel are necessary to meet the needs of a diverse community. We have found that both school and public librarians have a keen sense in determining what content to present to their students and community. We are also seeing that they can create easy to understand Internet access rules based around easy to understand criteria that empowers parents with choices.

By way of example, Library "A" installs LibraryGuardian around these rules:

- Level 1 Completely Unrestricted Internet Access
- Level 2 blocks Graphic and Extreme Pornography
- Level 3 blocks Graphic and Extreme Pornography, Sex, Hate Speech
- Level 4 blocks Graphic and Extreme Pornography, Sex, Hate Speech, Criminal Skills
- Level 5 blocks Criminal Skills
- Level 6 allows KidsClick! and Awesome Library only

Where Library "B" installs LibraryGuardian around these rules:

- Level 1 Completely Unrestricted Internet Access
- Level 2 blocks Graphic and Extreme Pornography
- Level 3 Library own created list of Web Sites.

Of importance is that the library did its job in providing information on the Internet usage policy and what is expected from each level and then handed the responsibility to the parents for them to decide what they wanted for their own children.

The parent or guardian has the ability to select a level that they believe is in the best interest of their children. The librarian understands the diverse cultures in their community. Tools that allow the two to work hand in hand are a viable solution to true community based Internet access management.

LibraryGuardian is architecture is designed to facilitate for certain checks and balances. Within the public system, LibraryGuardian does not block returns to a standard search engine like Yahoo!, Excite, Lycos, to name a few. Depending on the access level as selected by the parent, the child may not be able to access the links from the search. This "feature" insures both library and patron that all addresses and links to web content can be identified and challenged against the policy if necessary. If a site is wrongly blocked, the librarian has the tools to make the correction immediately without turning off the system or disrupting others currently online.

Problem #2: Patron delivery of web content without segregation of computer assets or password sharing.

Enter the SmartCard: A credit card-sized card with an embedded microprocessor chip. The SmartCard is at the heart of LibraryGuardian and provides secure IP independent authentication of a card user anywhere on the Internet. Other than the SmartCard, an inexpensive SmartCard reader is the only other required device to access the Internet.

When a patron registers for Internet access, they receive a SmartCard. This card can also serve as the library's patron card or school ID; for example imagine your current library card with a small brass contact on one of its sides. When the card is registered with the LibraryGuardian system, the LibraryGuardian servers will associate a unique secret serial number on the SmartCard with the cardholder's self-made password.

The LibraryGuardian registration is instant and the patron can access the Internet immediately.

The Patron may go to any Internet terminal in the facility designated for public usage. Upon first sitting down to the terminal, the patron may find several pages of web content that can be accessed without using the card.

We discovered that many libraries and public facilities have home pages that include links to areas like, "Crime Stoppers", "Contact your city or county elected officials". We felt it would be in the patron's best interest to access such pages without having to authenticate or even register. Suppose you have a creative idea for your Mayor, we felt that the message would be diluted if you first had to register. So the library has the ability to designate Internet usage that is accessible without use of a SmartCard.

The SmartCard comes into play when the user attempts to access the "open" Internet. On each page request, the servers carefully check the control lists against the access rules of the current user. If the site is accessible for the level prescribed by the SmartCard - Access Rules combination, the site is viewed on the terminal. If the site is not allowed, a simple text screen is displayed with a message provided by the local library. LibraryGuardian keeps no lists, and does not report on either access granted or denied. It is our opinion that keeping this information private is of utmost importance to both the patron and to the growth of the publicly accessed Internet. It should also be noted that the patent filed for LibraryGuardian in 1999 covers the methodology of handling this rule and is able to accomplish this objective without diminished speed of the Internet connection.

With the SmartCard solution, the Library patron is free to use any Internet connection that has the LibraryGuardian client software (approximately 150k in size). In other words, with all systems and databases residing securely on the Internet, the "parental rules" are completely portable from the Main Library to other branches, school, home or other places of public Internet access.

Problem #3: Handling other "pitfalls" in public access areas.

The public library is also confronted with problems such as patrons leaving "Adult Content" present on computer screens at the completion of a session. In many instances, this has been intentional to the dismay of parents approaching public terminals with small children. In discussion with several libraries, this was one of the deciding factors to filter patrons.

The LibraryGuardian SmartCard must remain present in the SmartCard reader for the entire Internet session. When patrons are finished, they must remove their SmartCard, which initiates the computer shutting down all open browsers, clearing the cache and restarting a fresh browser window. In essence, each new patron, irrespective of the time of day, will access a "clean computer". This feature assures administrators of public machines that they will have less worries about the content viewed by adults, which in turn helps with the policy decision to allow "Unrestricted Access" as a manageable asset to their patrons. This feature facilitates a better sense of privacy for all patrons in public areas due to the staff not having to follow behind each and every patron to check computers.

Having a required SmartCard present means that patrons can't authenticate themselves and then simply hand the card to another person to gain access to the Internet. With what we refer to as "secure two factor authentication", LibraryGuardian helps to remove the "warm fuzzy" feeling of protection where people simply share passwords and other methods of authentication.

LibraryGuardian also enforces other critical policy matters such as the total amount of time per day a patron can access a public terminal, cash to card features that include paying for printing and other services in a private manner as well as delivering digital signatures to open up new opportunities for a safer Internet for those that use public access. We are constantly improving and enhancing LibraryGuardian to be a toolkit that assists parents in providing value-based Internet rules for their children and helps bridge the digital divide by providing a server based service that causes a public terminal to have a more "home-like feel" for the user.

In closing, I believe that child safety is but one important issue for the global usage of the Internet being accessed in public facilities. What we have tried to accomplish with this technology is to empower parents with the tools to help them "parent" in this emerging digital age and provide a way for a community to offer a viable service to all ages. In creating LibraryGuardian, we had confidence that through technology we could provide an Internet solution that is not just an answer for families, but also a solution that could forge the integration of tools that enable public facilities to bridge the technology divide for those that rely on public access as their only means to the rich content of the World Wide Web.

Respectfully Submitted,
July 20, 2000
Stephen L. Boyles

BRIEF: **Michael R. Stephani**

B. S. in Management Science
Lockhaven University, 1985

Home: Elmira NY

President/Chief Executive Officer
Exotrope, Inc.

Michael, together with his brother and two of his friends created the Internet service provider that was incorporated on December 2, 1997. Since its inception, the company has grown to a globalized organization with approximately 90 employees within its umbrella. The umbrella includes EIS Global, EdNext$^{(TM)}$, InterFaith Net$^{(TM)}$ and The BAIR$^{(TM)}$ Filtering Systems.

Consultant
Stephani Dairy Service

Before his career with Exotrope, Michael served as a consultant to *Stephani Dairy Service*, owned by his brother, Kevin. Mike created a marketing program that successfully generated the greatest number of unit sales for automatic milking machines, exceeding sales of all other Alfa-Laval dealerships in the United States.

Proprietor
Stephani Chemical Company

In 1992, Michael began the *Stephani Chemical Company*, which dealt in bulk chemical sales. While president of the company, he made the largest sale of industrial cleaning solvents in the New York State area; furthermore, his company's single largest contract was to the NYC Transportation Authority. Other essential transactions included sales of industrial washing machinery parts to such companies as Arrowlock and Ingersoll Rand. In late 1997, Mike sold the company for an undisclosed amount of money.

Account Manager
Sales Support Specialist
Paxar Corporation

Between 1986 and 1992, he was employed with *Paxar Corporation*. Michael joined the company as a Sales Support Specialist where he enlisted in a special two-year management-training program. Michael completed the program within eleven months, during which time he learned every facet of the company from production to management

Michael achieved a special honor during his career with *Paxar*. In 1996, his test score from the Otus Intelligence Exam was the highest in the history of the company, further proving his aptitude for detail and quick, correct decision-making.

Michael was given the task of Project Coordinator for the "640 Program"; a thermal transfer bar code printer for textile and apparel manufacturing applications.

The position coordinated the new high-tech machinery with a myriad of supplies and peripherals, ensuring total compliance of all parts and supplies. Responsibilities encompassed the assessment of each step of the manufacturing process; in addition, he supervised the melding of three manufacturing plant locations which had no prior association, and neither had processes in place to facilitate the new co-manufacturing effort.

The project was successfully completed on time and as a result, Mike was given the opportunity to support any sales territory in the company. His choice was New York City for its competitiveness, opportunities and income potential. In less than four years, his territory sales more than quadrupled.

Business Manager
Penn-York Opportunities

While employed with the non-profit, sheltered workshop, Mike implemented new marketing research and methods; these procedures remained in place as th

The BAIR technology utilizes an advanced neural network of our company's own design. "BAIR" is an acronym for Basic Artificial Intelligence Routine. The BAIR technology is a server-side application that utilizes an innovative pattern recognition engine to ferret out pornographic **images** as well as text and block them on-the-fly from download from an ISP's servers. BAIR technology is just now widely being deployed in countries as far away as the United Kingdom, Italy, Australia, and Hong Kong. BAIR is available to Internet service providers, households, schools, and businesses in all fifty states.

AOL Foundation IEI Blue Ribbon Panel

Ginny Wydler
Director, Standards & Policy
America Online, Inc.

As Director, Standards & Policy, Ginny is responsible for a broad variety of policy considerations aimed at ensuring consumers have a safe, enjoyable experience with AOL's products and services. Her role encompasses child safety and privacy protections (including AOL's Parental Controls), advertising and content standards & practices.

Ginny joined AOL in 1994 in business development, growing and developing AOL's children's programming, launching the Teens and Families channels and helping to evolve AOL's Parental Controls. She was AOL's spokesperson for the Internet Driver's Ed program, a national traveling Internet education and safety class for children and parents, and was selected to serve on the Blue Ribbon Panel for AOL Foundation's Interactive Education Initiative for the three years since its inception.

Prior to joining AOL, Ginny worked in several positions at The Walt Disney Company, including film marketing and consumer products licensing. Ginny received her MBA from the JL Kellogg School. She has been active with children's educationall programs for many years - participating in Chicago Cities in Schools program and tutoring at elementary schools. She and her husband are now busy with their own young son.

Testimony of Ginny Wydler
Before the COPA Commission
At its Hearing on Filtering and Labeling
July 20, 2000

As Director of Network Standards and Policy for AOL I am responsible for a broad variety of policy considerations aimed at ensuring consumers have a safe, enjoyable experience with AOL's products and services. This includes responsibility for our child safety and privacy protections (including Parental Controls) and general advertising and content standards & practices. AOL is pleased to be represented on the COPA Commission and involved in its efforts as we work toward our mutual goal of finding the most effective ways to protect children online.

Our mission at America Online is to build a global medium as central to people's lives as the telephone or television… and even more valuable. We want to build a medium we can be proud of. America Online has played a significant role in the development of the online medium and we have always shared a special appreciation of its enormous power to benefit society - especially kids.

Learning how to explore and understand the online world is an essential skill for our children in today's wired world, but we all agree that kids need and deserve special protection in this new medium. That is why we at AOL have placed such a strong focus on making our service and the online medium safe as well as rewarding for children. By integrating cutting-edge technological tools, promoting major public education campaigns, and closely cooperating with elected officials and government agencies, we have tried to offer strong proactive leadership in every area of children's safety online.

In some ways even more important than those efforts, however, has been our work to provide our member families with the resources and tools they need to make informed decisions. No law, no technology, no corporate initiative can ever take the place of an educated and involved parent when it comes to their children's online safety. That's why we've dedicated significant energy to providing AOL parents with the most useful information, content, tools and safety tips to help protect their children, as well as a list of the resources available for families both on AOL and the Internet. By doing so, we've tried to empower parents so they can reinforce the rules of online safety, pay attention to what their kids are doing, and make use of technology such as our Parental Controls to protect their children from inappropriate content.

Industry Efforts to Educate the Public

We have always believed that the industry must lead efforts to give parents the tools they need to protect their children online. Equally important to offering parents choices online and great content for children is ensuring we continually educate consumers about Internet safety. AOL has been an industry leader in organizing industry efforts to educate consumers about online safety and will continue this leadership.

Among those efforts, AOL was a leading corporate host of the America Links Up national public education campaign, designed to give parents information to help their children have a safe, educational and rewarding experience online

In addition, AOL created and distributed a special video for kids called Safe Surfin' that features online safety tips from some of the younger generation's favorite celebrities. It was developed in partnership with the National School Boards Association and has been introduced into schools across the country.

And AOL, in conjunction with the American Library Association, launched the Internet Driver's Ed program. This program is a traveling Internet education and safety class for children and parents, hosted in children's museums and other prominent venues in major cities nationwide.

AOL works closely with the National Center for Missing and Exploited Children (NCMEC) to support its mission of recovering missing children. Since July 1997, AOL, our subsidiary Digital City, and NCMEC have maintained an online program called "Kid Patrol" which helps locate abducted and missing children. AOL also helped to launch NCMEC's Cyber TipLine.

And AOL was a key partner in forming GetNetWise.org to provide consumers with comprehensive online safety information through links from both the AOL subscription service, AOL.com and Netscape.

Ongoing Education of our Members

We have found that education of our members is an ongoing process. As new consumers come online every day and as our existing customers' lives evolve, their parental controls needs may change as well. AOL members spend an average of 60 minutes online per usage day (Source: Media Metrix Digital Media Report, April 2000 Home/Work), so we have ample opportunity to remind parents about their choices, and about online safety. This is important not only for new members to our service, but for existing parents as well. We believe that every family should periodically review new information, check their child's Parental Controls settings and update them as appropriate for that child's age and maturity. Also important, we have worked to quickly and effectively notify our members of significant news and developments in the area of children's safety, like the Children's Online Privacy Protection Act or new Parental Controls offerings that may impact their family's online safety decisions.

We reach our members through several key vehicles online. Neighborhood Watch and Parental Controls are our central "online safety" information areas. These areas are always available online to our members through easy-to-find/navigate mechanisms including:

1. Keywords: We use logical "keywords" such as "child safety," "parental controls," "safety," "Note to Parents," and "help" to lead our members to online education areas about child safety and privacy. Online safety for kids is a topic in our AOL Help A-Z area. And we educate our newer members about keyword use early on, through Welcome Screen promotion of our Member Benefits Area.

2. Prominent Placement: Parental Controls is an icon on the Welcome Screen of our service which each member passes through each and every time they sign online. Additionally, Parental Controls are integrated into our Create A Screen Name process.

In addition, our service provides the opportunity for frequent updates through:

3. Kids Only & Teens Channels Reminders: Both our Kids Only channel, targeted to children 12 and under, and our Teens channel, targeted to younger teens 13 to 15, have online safety tips integrated into the experience. In fact, kids and teens must pass through these safety reminders before entering interactive chat and message board areas.

4. Steve Case Community Updates: These updates, which receive prominent, ongoing promotion on AOL's Welcome Screen, frequently focus on child safety. April's letter, outlined child privacy protections, reminded parents to create separate screen names for each child and highlighted additional online resources for more information and help.

5. Parental Controls promotions. Parental Controls are promoted frequently through high trafficked areas including our new "Member Benefits" area, member orientation online and banner rotation in the "Read E-Mail" form. In one such recent promotional campaign on our service, Parental Controls banners received an average of over 42 million ad impressions each month.

Engaging Content for Children

An essential part of AOL's commitment to families is to provide great content for children. Providing entertaining and educational experiences for kids has always been an important mission for America Online. The AOL Service reaches over 2 million children ages 2-11 (Source: Media Metrics, May 2000). For over 7 years now, AOL's Kids Only channel has been delivering fun, engaging and educational programming to children 12 and under. The channel receives accolades from the kids (and their parents) who visit and engage in it in ever increasing droves.

AOL holds itself and its content partners to the highest standards to deliver a safe, rewarding experience for children. To do so, we developed and codified strong institutional protections into AOL Kids Policies and AOL Teens Policies to which each of our partners must adhere. These policies, in addition to outlining privacy protections that must be in place for each audience, also outline baseline content standards for each area. Each of our content partner sites is reviewed by our third party web filtering company, The Learning Company, for addition to the "white list" of sites as age appropriate for Kids Only screen names and/or Young Teens. Additionally, each partner in our Kids Only channel must fully monitor chat and message board areas to ensure they remain age appropriate.

AOL's Parental Controls

AOL's Parental Controls are the foundation of our child protection package and a key offering of our service. While providing kids with entertaining and educational experiences has always been an important mission for America Online, we strongly feel that it is also our responsibility to help parents manage their child's online experiences. AOL's Parental Controls put the power in the hands of parents, enabling them to make informed decisions about their kids' online activities by selecting the appropriate level of participation for each child. Parents also have the ability to customize additional features - such as chat, email, and Internet access - based on their children's online savvy and maturity.

Parents love the fact that AOL's Parental Controls are so easy to use. In fact, our members ranked Parental Controls among the top 8 features of our service. And children love having their own personal screen name and the special content developed just for them.

AOL's Parental Controls are a server-based technology. This delivery mechanism allows us to provide the most secure experience to our users because the Parental Controls settings are actually attached to the child's individual screen name. No matter where that child signs online -- from home, school or a friend's house, the Parental Controls follow.

In 1998, we changed our registration process to require parents to set Parental Controls for each screen name upon registration. When we integrated Parental Controls into the Create A Screen Name process; we saw a dramatic increase in adoption as a result. There are up to 7 screen names available on one AOL account, enabling even larger families to give each child in the household his or her own screen name with customized Parental Control settings. Only "Master" screen names controlled by the parents can create a new screen name or set or change Parental Control settings.

When creating a separate screen name for their child, a parent is given the opportunity to choose one of three different standard age "category" settings:

Kids Only, Young Teens, or Mature Teens. (They also have the option of classifying the account as General Access, which has no Parental Controls).

A Kids Only setting (recommended for 12 and under) restricts children to the Kids Only channel, which has been specially created and programmed for children 12 and under. The child also receives a customized Welcome Screen. A child using a Kids Only screen name can access age-appropriate content on AOL and the Web and interact with others online through e-mail and in special supervised kids' message boards and chat areas, but is blocked from taking part in general audience chat rooms and message boards, sending or receiving Instant Messages and visiting any web site that has not been reviewed and approved as age-appropriate.

A Young Teen (recommended for ages 13 – 15) category provides more freedom than a Kids Only screen name, but does not provide full access to more mature content and interactive features. Young Teen screen names can access most AOL content, and can visit Web sites that have been reviewed and approved as age appropriate. They may communicate with others online through e-mail and in a range of message board and chat areas. They are restricted, however, from accessing news groups, visiting inappropriate web sites, exchanging Instant Messages or taking part in private chat rooms. A Mature Teen (recommended for ages 16-17) setting allows older teens the most freedom of any of the Parental Controls categories. Mature Teen screen names can access all content on AOL and the Web except sites that have been classified for an adult (18 plus) audience. They can locate others and communicate online through Instant Messaging, all chat areas, e-mail, private messaging and AOL's Member Directory.Each of these category settings has a pre-selected set of "defaults" for different features such as chat, e-mail, Instant Messages and Internet access. A parent can choose to customize any of these defaults within a category to ensure the experience best matches his or her child -- so even on a Kids Only account (our most restrictive), a parent may choose to further limit access to e-mail to an "approved" list, or, alternately, may decide that the child is mature enough to participate in Instant Message conversations. Because each account is tied to a specific screen name, we can ensure that no child with Parental Controls is allowed to access a particular content area or participate in a chat until the Parental Controls information for that account has been checked against our database. When a child types in a website address or clicks on a web link, AOL checks the Parental Controls information attached to the screen name, and based on the category, makes sure that the site is on the approved list before allowing it to appear.

We created separate categories for kids and for teens because we understand that maturity levels vary widely at these ages. We offer two teens settings to accommodate our members' interest in differentiating a 13–year-old's online experience from that of a 16 to 17-year-old.

After selecting a Parental Controls category for their child's screen name, a parent may further customize or modify their child's activities through Custom Controls. A parent may choose to modify their child's access to content (Web, newsgroups, file downloads) or way to communicate with others online (email, Instant messages, chat). For example, if you have a ten-year-old child who you want to only allow to exchange email with a list of specific friends and relatives, you can customize Parental Controls to only allow e-mail access to people on that list.

While there has been much focus on protecting children from email, another Internet function that raises special concerns for children is instant messaging. While instant messaging is wildly popular with children who create their own online communities of friends, there are unique issues raised by this feature which allows people to chat in real time. On the AOL service, IMs are default "off" for Kids Only and Young Teens screen names because we want parents to understand and consciously decide that this one-to-one communication is appropriate for their child.

Evolution of AOL's Parental Controls

Parental Controls have been integrated into the AOL service nearly since its inception. Our Parental Controls have always, and will always, continue to evolve in response to consumer demand. Our early feature set focused on "products" -- allowing consumers to fine-tune their child's experience by selecting essentially "on or off" functionality for a variety of features including chat, newsgroups and e-mail. We developed the "Kids Only" category setting in 1995, recognizing the increasing popularity of our children's content, and the increasing number of families getting online. As the online medium became more mainstream, we focused on simplifying our Parental Controls. In 1997, we added our two "teens" categories, for parents who wanted a "one button" solution to setting controls. Even so, we continued to offer fully customizable selections for those parents who wanted to customize their child's experience. This "category" approach has proven very successful and popular with our millions of families with children.

We continue to evolve our Parental Controls to meet consumer needs for safe, easy to use tools. In response to consumer request, we recently introduced our latest feature, the Online Timer, in Spring of this year. This feature allows parents to determine how long and when their children can be online, and was among our most highly requested features.

In addition, we recently introduced a Teen Search product that enables an age appropriate search experience for teens, available through our Teens channel, or kw: Teen Search. We are working with a broad number of organizations including the American Library Association, and GLAAD to ensure that a diversity of voices and views are taken into account as this product is developed.

We will continue to enhance our web controls by working closely with our partners to ensure the broadest range of age acceptable sites are accessible to children and teens, and to minimize the possibility that inappropriate content will get through.

Our Process to Resolve User Complaints with Parental Controls

No system is perfect, so we encourage our members to continually provide input to make our Parental Controls better. Consumers have direct input to request that a site or sites be reviewed for addition to or deletion from a particular category of access. This functionality is available at kw: Web Request and also available at kw: Parental Controls. We receive over 400 requests per week through this mechanism. Through our members' valuable input and suggestions, the Learning Company can better evaluate what places are age-appropriate for each group. However, we also recognize that what one parent may find objectionable another may find perfectly acceptable, and that's why we offer varying levels of web controls.

One commonly heard criticism of filtering is that the technology can often overfilter. We do hear from our members that the smaller sites sometimes are not accessible to their children on Kids Only and Young Teen (or "approved list") settings -- for example "Johnny's school soccer site" might not be available. By encouraging our members to submit those smaller sites through the Request a

Site mechanism, we try to ensure that as many web sites as possible have been reviewed and approved.

Games Rating

One area where we have chosen to rate is on our Games Channel. Last fall, as part of our commitment to provide parents with information they need to guide their child's online experience, AOL endorsed the Entertainment Software Rating Board (ESRB) rating system for online games. All AOL games carry an ESRB rating, and we are working with the ESRB to develop a task force to garner support for and address challenges with online game ratings and to address the particular challenges of online environment.

International Implications of Child Online Safety

The ability to seek out information and resources across international borders is one of the benefits of this medium for our children, and we want to ensure that parents around the world have the ability as our U.S. members to guide their children's online experience. That's why AOL has always integrated our Parental Controls technology into each our International services, which now number fifteen.

What has been most interesting to us as we have taken our Parental Controls "international" in launching local versions of the AOL service in other countries is that a one size fits all approach to child safety does not work. While every country shares the common goal of protecting children from inappropriate content, each country also has unique standards regarding what parents believe is inappropriate for children. Despite those valid national differences, we are concerned about the increasing efforts by some countries to enact restrictive local laws on Internet content. If this trend continues, we run the risk of creating an unworkable crazy quilt of global regulation that will hinder the growth of the medium and undercut our common goal of protecting children. Of course, all of these issues will only intensify and become even more important as global Internet usage grows.

Conclusion

To briefly summarize, AOL's commitment to families and child safety includes three key elements: educating consumers about online child safety, including our collaborative efforts with other companies in the industry; providing great age-appropriate content for young audiences; and offering parents easy to use, flexible tools to customize their children's online experience.

We are constantly enhancing our offerings to families and work closely with others in the industry to fine-tune our technological tools so that they are the most up to date and effective. Filtering, rating and labeling technologies are essential parts of the toolkit that can be used to protect children on the Internet.

Finally, it bears repeating that there is no substitute for parental involvement online. Raising consumer awareness about parental controls, choices and child online safety is a collaborative effort. AOL believes that the industry and we have made great strides in this arena and are on the right path to continue doing so.

TIMOTHY B. ROBERTSON

Tim Robertson currently serves as Chairman of Bay Shore Enterprises, LLC, an investment holding company with activities in international media and Internet technology ventures. Its most significant investment is in FamilyClick.com, LLC, an online service provider dedicated to offering safe and filtered Internet access for families. He most recently served as President and CEO of International Family Entertainment (IFE), which was best known for its flagship cable network, The Family Channel. IFE was acquired by Fox Kids Worldwide, Inc. (FKW), in September 1997, and is now a wholly owned subsidiary of FKW.

After taking IFE public in 1992, Robertson built The Family Channel into one of America's most watched cable networks. The company also grew to include MTM Entertainment, Inc., a company involved in development, production and distribution of television series and other programs throughout the world; FiT TV, the only 24-hour cable network dedicated to health and fitness; and United Family Communications, a joint venture with United International Holdings.

A leader in the cable industry, Robertson has brought a vision to family television that has influenced the marketing of cable to a nation with shifting values. He has targeted the emerging American family with sophisticated programming that includes original films, specials, syndicated programming, and comedy and drama series.

He has served on the boards of a variety of cable and industry groups such as the National Cable Television Association where he received its prestigious Vanguard Award for Young Leadership in 1992, the Cable Television Advertising Bureau, the Walter Kaitz Foundation, the National Academy of Cable Programming, and Cable in the Classroom.

Robertson is currently on the Board of Visitors for University of Virginia and is a recently appointed member of the Governor's Blue Ribbon Commission on Higher

-more-

Education in Virginia. He also serves on the Board of Trustees for Regent University, the Board of Trustees for Norfolk Academy and the Board of Trustees for the DON'T QUIT! Foundation, and he has been appointed to the boards of the Children's Health Foundation and Virginia Marine Science Museum. He is also a member of the Arts and Sciences Alumni Council for the University of Virginia and has served as past campaign co-chairman on the United Way of Virginia Beach and on the Board of Directors of Operation Smile.

A graduate of the University of Virginia with a Bachelor of Arts in English, Robertson also received a Master of Divinity degree from Gordon-Conwell Theological Seminary and completed the Executive program in Business Administration at the Graduate School of Business, Columbia University. He and his wife, Lisa, have four daughters and a son and reside in Virginia Beach.

###

FAMILYCLICK™
Connecting Families

Commission on Online Child Protection (COPA)
July 20, 2000

Prepared Statement of Mr. Timothy B. Robertson
Founder, Chairman, President and Chief Executive Officer
FamilyClick.com LLC
2877 Guardian Lane, Suite 300
Virginia Beach, VA 23452

Members of the commission, distinguished guests, I am Tim Robertson, Founder and CEO of FamilyClick.com LLC; a nationwide Internet filter provider based in Virginia Beach, VA. I would like to thank you for the opportunity to speak with you today about the subject of protecting our children from the offensive material and predatory activity that is so prevalent on today's Internet.

I have personally been involved for a number of years with delivering family oriented programming, information and entertainment through the media. Before forming FamilyClick, I served as the President and CEO of International Family Entertainment (IFE) which was best known for its flagship network; The Family Channel. With its commitment to wholesome, family oriented programming, The Family Channel grew into one of America's most watched cable networks. In 1996, I served on the task force created by the National Cable Television Association to help craft the Television Parental Guidelines. In 1997, IFE was sold to Fox Kids Worldwide for $1.9 billion.

Now, we are doing the same for the Internet as we did with cable. The same creative team that brought The Family Channel into America's living rooms has now created FamilyClick; a total solution that provides safe Internet access as well as a dedicated web site offering compelling and original family oriented content. By combining the best technology that industry has to offer with our own extensive in house experience and expertise, FamilyClick offers families the same peace of mind while browsing the Internet that The Family Channel brought to their television.

The Problem

The Internet has tremendous potential for today's children. Children today can access information that was out of reach just a generation ago. Through the Internet, reference material located on the other side of the world is just as close as the library around the corner. The Internet allows children to explore new worlds, meet new people and develop new skills. Never in history have children had access to such a powerful tool for learning, entertainment, communication and exploration.

But the Internet is also fraught with perils. Almost everyone has heard stories of grown men posing as teenagers in online chat rooms. According to a recent survey funded by the National Center for Missing and Exploited Children (NCMEC)[1], one in five children between the ages of 10 and 17 has received a sexual invitation or approach on the Internet in the last year. One in thirty-three received an aggressive sexual solicitation. One in seventeen reported having been harassed or threatened over the Internet within the last year. One quarter of the young people reporting these incidents were distressed by them. And, not surprisingly, most incidents involving young people go unreported.

Many of us know someone who may have accidentally stumbled across a pornographic web site; perhaps some of us have had that unfortunate experience. Many of us have also received an unsolicited email message containing pornographic or otherwise offensive content. It is estimated that at least fifty-three percent of America's teenagers have encountered web sites featuring pornography, hate or violence[2]. One in four have unwillingly accessed pictures of naked people or people having sex[3]. More than sixty-two percent of parents of teenagers are unaware that their children have accessed objectionable web sites[4]. There are more than 40,000 individual URL's containing child pornography, pedophilia or pro-pedophilia content[5] and U.S. News and World Report states that there are at least 40,000 porn sites operating on the web today[6]. Actually, if it were possible to count them all, that number would be much higher. And at least 30 percent of all unsolicited email messages contain pornographic information[7].

The statistics are alarming. But, the numbers do not tell the whole story. If we were to count the number of adult bookstores or the number of pornographic movies available today, we might come up with similar numbers. Pornography has a foothold in almost every segment of society, ranging from the red light district on the other side of town to the back room of your local video store. There have always been people seeking to prey upon young, innocent children. We all know that pornography is out there; it always has been and probably always will be. On the Internet, the problem isn't so much that pornography exists. The problem is the way in which online pornography is often intrusively marketed and the ease with which predators can access our young people.

You would probably be up in arms if your teenage son or daughter went out to get the mail and carried in a piece of junk mail containing a graphic advertisement for a recently released triple X rated film. You would most likely call the Postal Service or other authorities and demand that some type of action be taken. And action would be taken because there are laws and regulations that prohibit the distribution of pornographic material in that manner and those laws are aggressively enforced. Because of the enforcement of such laws and regulations, you are very unlikely to receive such material in the mail.

---

[1] National Center for Missing and Exploited Children, Online Victimization: A Report on the Nation's Youth, June 2000

[2] Yankelovich Partner survey, The Safe America Foundation; 9/30/99

[3] National Center for Missing and Exploited Children, Online Victimization: A Report on the Nation's Youth, June 2000

[4] Yankelovich Partners Study, September 1999

[5] Safeguarding Our Children-United Mothers & CyberAngels "Our Kids In Danger List," 2000

[6] U.S. News & World Report, 3/27/00

[7] Choose Your Mail.com study, October 1999

But you are actually very likely to receive such an ad in an unsolicited email message. Someone who delivers pornographic or otherwise offensive material to your electronic mailbox is very unlikely to face legal action. The online pornographer is well aware of that fact. Using easily affordable bulk email software and an equally affordable mailing list, the online pornographer can quickly and easily get his message across to thousands, if not millions, of users. And these are far from being targeted mailings; the bulk mailer is simply interested in getting his message sent to as many people as possible. Your ten year old son is just as likely to receive such a message as is a 45 year old man.

While channel surfing in front of your television, how likely is it that you will stumble across deviant material like bestiality or child pornography? Not very. You are also very unlikely to accidentally catch a how-to show explaining the intricacies of constructing a bomb or a show asking that you send in your donations to a white supremacist group. Again, enforcement of broadcast regulations protecting you from this type of material serves as a deterrent to such abuses. Your cable or satellite provider knows very well that the switchboards will light up if any inappropriate programming somehow 'sneaks' in.

Even though some television programming today may not exactly qualify as family fare, you feel somewhat safe when sitting in front of your TV. You should not feel safe when sitting in front of a computer with unrestricted access. Web sites dealing with all types of pornography, hate, violence and other inappropriate subjects are readily available. These sites often hide behind deliberately misspelled or innocent sounding domain names such as www.whitehouse.com, www.watersports.com, www.boys.com and www.dinsey.com. Recently, children who had trouble spelling the word Pokemon ended up going to a graphic pornographic web site. The online porn industry has become adept at deceiving and luring people into visiting their web sites.

If a teenaged boy or girl walked through the front door of an adult bookstore, accidentally or otherwise, he or she would most likely be escorted back onto the sidewalk in a matter of seconds. But not in cyberspace. A visitor who wanders into the web's dark side is likely to be held hostage for as long as the porn operator can get away with it. Almost by reflex, we have been conditioned to hit the Back button on the browser when we want to leave a web site. But hitting the Back button to leave a porn site quite often results in the opening of another browser window featuring a suggestive, if not graphic, site. The reluctant visitor often leaves an adult web site by way of a dozen or more other offensive sites. In many cases, the attempt to leave an adult site results in the simultaneous launching of many new browser windows; each featuring a different pornographic site. This often locks up the user's computer, resulting in a necessary reboot.

Employing methods meant to deceive, lure, tease, trick and capture, porn operators can generate a steady flow of traffic to their site in a fraction of the time that it takes a legitimate web site to build the same amount of traffic. The methods that the online porn industry uses to attract business would not be tolerated away from the Internet. But in cyberspace, the rules of engagement that are allowed are vastly different.

The scope of the problem and the aggressive nature of those who would use the Internet to prey upon our children are why parents are demanding a one-stop shop service like FamilyClick. That is what drove us to create FamilyClick. We commissioned various market studies not only to judge the demand for a solution but also to help us understand parent's awareness of the problem. We found that 72% of wired homes with children agreed that objectionable materials on the Internet were a major problem and that 54% of homes with children expressed an interest in a solution such as that proposed by FamilyClick. Parents desire a complete technical solution that would provide worry free access to the Internet, the ability to unobtrusively monitor children's web activities and protect them against unsolicited e-mail.

The FamilyClick Internet Safety Philosophy

When we started FamilyClick, we began with a commitment to provide families with the safest Internet experience available on the market. To meet this commitment, we conducted extensive research into the dangers of the Internet, we consulted with the leading experts in the field, we carefully evaluated existing solutions to the problem and we assembled a talented team of engineers, content creators and technical experts with proven track records. Our goal was, and continues to be, to develop a total solution that would provide families with safe, cost effective and worry free access to the Internet.

Our initial aim was to identify and acquire the best existing solution and to add our own in-house expertise in order to create the FamilyClick service. We carefully examined a number of filtered Internet service providers and found that most of them lacked flexibility. The same level of filtering applied to the teenagers was also applied to younger children as well as to the parents. We quickly determined that content that is appropriate for an adult or older child is often not appropriate for younger eyes. We decided that the FamilyClick solution had to be flexible and allow the parents to customize the degree of filtering based on the maturity level of the member that is online. Rather than offering a 'one size fits all' solution, we wanted the decision of determining the access levels of children to stay where it belongs: with the parents.

In many of today's households, the kids are more computer literate than the parents are. It is quite common for a parent to purchase a software package for the home computer and hand it to one of the children to be installed. Desktop filtering systems, which reside on the users computer, are vulnerable to tampering by technically savvy teens. Simply modifying the proxy settings within the browser can often disable server based filtering solutions. We determined that the FamilyClick solution had to be tamper resistant.

Very few of the filtered Internet service providers that we looked at had any significant market share. Instead of finding the AOL of the filtered access market, we instead saw a number of small niche players, often serving specific areas of the country. We were, in fact, surprised at how many people had actually attempted to offer a solution for families. Most filtered providers that we looked at lacked the strong brand identification that builds trust. It became clear that our technical solution had to be married with a strong marketing and educational program so that parents would be aware of both the problem and the solutions.

Just about every existing solution that we looked at concentrated on the web and completely ignored other protocols such as e-mail, chat and instant messaging, Usenet newsgroups and ftp. But most unwelcome sexual solicitations take place in chat rooms and message boards, unsolicited email messages frequently contain pornographic and offensive content and Usenet newsgroups are well known repositories of graphic material dealing with child pornography, bestiality and other offensive subjects. Filtering the web only solves part of the problem.

We live in a world where technology is advancing at a breakneck pace. In the time it takes to read this paper, someone will introduce a new time saving tool, a faster processor or a new network protocol. The online porn industry has historically been at the forefront of Internet technology; pioneering the use of streaming video and audio as well as community applications such as chat and instant messaging. Parents cannot possibly stay one step ahead of the porn industry; this has created a critical need for parent-industry partnerships like FamilyClick. As technology changes, so does the marketplace. High speed DSL access is now available to families that just a few short years ago accessed the Internet through a 14.4 modem. Companies that once thrived on selling access to the Internet now face stiff competition from competitors that provide access for free. Any effective solution that attempts to safeguard families Internet access must evolve to the changing marketplace and be able to quickly respond to new technological challenges.

The FamilyClick Total Solution

The FamilyClick Total Safety Solution offers cutting edge Internet safety by combining the best protective technologies currently available with our own proprietary safety technologies in order to build a "Superior Suite of Safety Services" and also delivers top quality, relevant content and entertainment to America's families. Our experienced team of Internet safety experts continues to evaluate and implement new technologies to ensure that FamilyClick remains at the forefront as an Internet safety service.

The FamilyClick Internet access service is a Plug-and-Play, one-stop solution that includes nationwide 56K-dialup access. In September, we will be introducing MyISP, which allows families that access the Internet via other providers to add the FamilyClick Total Safety Solution to their homes. FamilyClick MyISP will offer an unrestricted access level that will be password protected. Both products include the complete "Superior Suite of Safety Services" that makes FamilyClick the leader in the Internet safety market.

Safe Access

The FamilyClick Total Safety Solution begins with safe access to the Internet. Using server-based technology exclusively, FamilyClick offers families the assurance of modern, state-of-the-art filtering technology with the flexibility demanded by today's families. FamilyClick uses a comprehensive, multi-step filtering process to safeguard access to the World Wide Web as well as e-mail, newsgroups and chat. Our multi-step filtering technique ensures that dynamic material, such as web based email and search engine results, can be handled just as effectively as static web pages. Parents have full control over the level of access that their children have and optional features may be turned on or off quickly and easily. E-mail messages are subject to many of the same filtering processes that web sites are and our Smart Search Engine delivers only the best and most relevant results.

Web Filtering Technology: Our two step filtering process first compares a requested URL against an extensive list of reviewed sites. These sites are reviewed both manually and by automated processes and are categorized into approximately sixteen different categories ranging from crime and pornography to weapons and illegal drugs. PICS ratings, when available, are also used to categorize sites. Our substantial database of sites is updated no less than daily and additions, deletions and corrections can be made on the fly. The complete list of FamilyClick content categories is available in Appendix A.

The second step in our filtering process is a dynamic filtering process called ClickReview. ClickReview scans pages in real time and scores each Web page based on a review of the relationship and proximity of words to other words on the page. For instance, ClickReview can distinguish between a site on "breast cancer" and a site on "girls with big breasts," and treats the phrase "sexual harassment" differently from "sexual pictures."

Due to its dynamic nature, ClickReview is able to deal with dynamically generated web pages that other filtering technologies leave behind. FamilyClick's filtering process is just as effective on a web-based email account or with an HTML based chat as it is with a web page that never changes. And because the content of web sites changes frequently, ClickReview helps to ensure that 'safe' sites that might become 'unsafe' will not be displayed to our subscribers.

FamilyClick only provides access to chat rooms that are HTML based. This allows our ClickReview process to scan the conversation and screen out any inappropriate language that may occur. Unfortunately, to our knowledge, there is currently no technology available that can detect a disguised predator who does not use offensive language.

FamilyClick's World Wide Web filter combines industry leading technology from Symantec with FamilyClick's own technology to provide a web filtering solution unmatched in the industry.

Smart Search Engine: Safety must be combined with delivery of relevant and easily accessible content. For searching the web, FamilyClick has partnered with LookSmart to provide a powerful search engine that filters out offensive material and returns only the best and most relevant results. Our Smart Search Engine is integrated with our

ClickReview process to ensure that only sites that have passed through our layered filtering system are accessible via the search results.

FamilyClick members are also free to use any search engine they choose with confidence. As all results are subject to our ClickReview process, families can rest assured knowing that the search results will be free of offensive material.

Multiple Access Levels and Full Parental Control: FamilyClick realizes that different families have different needs and that children have different maturity levels. The FamilyClick filter allows parents to determine the level of access that is appropriate for each member of the family. Our access levels have been carefully designed to accommodate individuals of all age groups and parents can easily change the access level of any family member at any time.

For it's most restricted level, FamilyClick has developed the Children's Playroom. This is a 100% safe level of access recommended for children aged seven and younger. It allows access only to a pre-determined list of children's web sites that have been pre-selected and pre-approved by FamilyClick.

Our highest level of access provides protection against sites providing instructions on performing criminal activities, sites which advocate hate or intolerance, pornographic sites as well as sites advocating the use of illegal drugs, sites promoting online gambling and sites which advocate violence. In between, FamilyClick offers access levels appropriate for teens, pre-teens and older children. The complete list of FamilyClick access levels is outlined in Appendix A. FamilyClick's access levels allow parents to prevent young children from viewing material such as sex education while permitting access to older, more mature children.

It is FamilyClick's philosophy that parents and guardians are the best judges of what is appropriate for their children. FamilyClick offers parents complete control over the level of Internet access for each member of the family as well as access to features such as Usenet news, e-mail and personal web space. An easy to use web based interface gives parents the ability to add new family member accounts at any time and makes changing the access levels of individual family members quick and easy.

Filtered E-Mail: FamilyClick's world-class email service utilizes a two-stage system designed to identify and block spam and, optionally, scan incoming messages for pornographic or offensive content. At the first stage, the source address of each incoming mail message is compared against a database of known spammers. This database is updated in real time and is maintained by the well-known MAPS (Mail Abuse Prevention System) Project. This database includes the addresses of spam generators, open spam relays as well as potential dialup trespass spammers. FamilyClick also utilizes 'spam probes'; fake email addresses used to attract, collect and categorize unsolicited email messages. Our own list of well-known spammers is combined with the database provided by MAPS to provide one of the best barriers against spam available today.

If parents select FamilyClick's Mail-Block feature, the second stage scans incoming messages to detect pornographic or offensive content. Messages that break any of the content rules are returned to the sender and never appear in the users incoming mailbox. Parents can also decide whether to disallow e-mail messages containing attachments.

FamilyClick provides a fully featured web based interface to email which subjects each mail message to our two-step filtering process; filtering each message according to the access level of the recipient. Users also have the option of accessing their mail via the standard POP protocol using one of many popular desktop e-mail client programs. FamilyClick's e-mail service combines cutting edge software from Software.com with the time tested open source solution Sendmail to provide one of the safest and most effective e-mail solutions available today.

Newsgroup Filtering: Many users currently participate in Usenet newsgroups or discussion groups. HTML based news services such as Deja and Remarq offer users access to news, discussions and information covering literally thousands of topics. Because ClickReview has been designed to handle dynamically generated web pages, families can rest assured that the sometimes 'colorful' language found in these public discussion areas will not appear on their computer screens.

FamilyClick also makes available it's own news server which is accessible using any one of many popular NNTP clients such as Outlook Express or Free Agent. This news server carries a carefully chosen subset of the roughly 40,000 newsgroups that are publicly available and completely eliminates any groups dealing with pornographic, offensive or objectionable material. Articles sent to FamilyClick's news server are heavily filtered for offensive language and spam and any article containing a possibly pornographic binary image is rejected immediately. FamilyClick uses a proprietary password protected access control system to grant or deny access to its news server and parents have complete control over which of their family members have access to this service.

Instant Messaging Capabilities: FamilyClick allows users to access their favorite instant messaging packages including AOL Instant Messenger, Yahoo! Messenger and more. Although FamilyClick does not support these services, we provide safety instructions that may be applied to these and other instant messaging packages.

As with all aspects of the FamilyClick service, parents are given the option of turning instant messaging access on or off for their family and the default is always set to off.

Tamper Resistant Technology: The best protection in the world isn't of much benefit if it can be easily disabled. That's why FamilyClick has developed proprietary technology that helps ensure that the filter cannot be easily sidestepped. Users who dial into FamilyClick's ISP service are directly connected to FamilyClick's network; not to the Internet. Access to the Internet must be made through FamilyClick's array of filters. Families who use other access providers and choose FamilyClick's MyISP service are also protected against tampering by proprietary technology developed by FamilyClick engineers.

World-Class Technical Support: FamilyClick's service is designed to be easy to install, easy to administer and practically transparent in normal use. Once a user is logged in, the FamilyClick system operates quietly as a background safety net and makes its presence known only when it needs to block inappropriate content. In the event that questions come up or problems occur, FamilyClick has established a world-class technical support system designed to handle everything from the simplest question to the most complex problem.

No filtering system is 100% effective. Although rare, some sites that should be blocked are not. There are also sites that may be blocked even though they are perfectly safe and appropriate. Should such events occur, customers have access to FamilyClick's Site Review. By filling out a simple web form, customers can report sites that should be blocked or can request that we unblock sites that should not be. FamilyClick reviewers will respond to the request by the next business day and the user will get a response by email. If the reviewer cannot honor the request, the user will receive a detailed explanation. Due to the flexibility designed into FamilyClick's filter, corrections to the database can be made in a matter of minutes.

When a user has a question or problem, chances are somebody else has already asked the same question or experienced the same problem. FamilyClick maintains an extensive collection of FAQs (Frequently Asked Questions) on our web site. Answers to most of the questions that users may have are described in a language that even a novice user can understand. Solutions to problems that families may experience are presented step by step using a clear, concise, easy to understand format with screenshots and other illustrations.

For questions or problems that cannot be handled with FamilyClick's Site Review or online FAQs, we offer email support to all users. Questions or problems submitted by email to our support staff normally get a response in less than five minutes. And for those times when a user just needs to talk to a real person, we offer toll free phone support.

Top Quality Content

Identifying and filtering out inappropriate content is only half the solution. Families not only want to be protected from offensive and inappropriate material, they also want to know where to find compelling, educational and entertaining content that can be enjoyed by the entire family. To address this need, FamilyClick has designed its web site at http://www.familyclick.com as a starting point for families exploring the Internet. The FamilyClick portal is freely available to everyone online and features original content as well as articles from some of the most trusted and respected names in the industry.

Ten Channels of Family Oriented Content: FamilyClick has arranged the content on its web site into distinct channels including ParentingClick, MoneyClick, SportsClick, KidzClick, TeenClick and LearningClick. In all, FamilyClick offers ten channels featuring original content as well as material from such respected names as Dr. Paula, Body By Jake and the Weather Channel. FamilyClick has featured articles by noted authorities like Dr. Katherine Kersey of Old Dominion University. In addition, each 'click' features a moderated message board where users can post questions and comments.

TopClicks Points Users in the Right Direction: Because one web site cannot possibly cover everything, FamilyClick's TopClicks section includes lists of reviewed and approved "best of the Web" sites to help families find appropriate sites covering almost every category of interest. Included in TopClicks are licensed "Net Mom Approved" sites which are personally reviewed and approved by Jean Armour Polly, the original Net Mom and author of The Internet Kids and Family Yellow Pages.

FamilyClick completes the Internet experience by offering such features as personal web pages, games, news and weather updates and stock quotes.

Besides offering what we feel is the leading solution available today, FamilyClick has undertaken a nationwide marketing program designed not only to promote our offerings, but also to increase public awareness of the problem. Our goal is to make the FamilyClick brand one of the most respected and trusted names in the Internet protection industry. Our first national television commercial, featuring Leeza Gibbons, aired in May during the season finale of the CBS series "Touched By An Angel". Through our sponsorship of the Nascar Winston Cup stock car driven by Kevin Lepage, the FamilyClick brand is gaining national attention and recognition.

Conclusions

We all have an important responsibility to help safely bring the promise of the Internet to America's youths while protecting them from people and influences that we would never let through our front door. As the provider of a private sector solution, FamilyClick is part of a three-prong solution that shares the responsibility between the public, the technology industry and the legal community.

Despite the increased publicity that Internet predators and online pornography have received recently, many parents are of the opinion that inappropriate sexual encounters on the Internet only happen to somebody else's kids. Like the children's faces on a milk carton, the young victims of online abuse are usually anonymous; never the kids across the street or the sons or daughters of a co-worker. Sadly, few of us take any action until someone close to us has been involved and then it's often too late.

FamilyClick believes that education, awareness and empowerment are essential in ensuring that our children can gain all the benefits of the Internet without being exposed to the dangers. Libraries, schools, parents, teachers, churches and every person and organization that has a role in our children's lives needs to understand their responsibility toward protecting our children from the aggressive tactics of online pornographers and from online predators.

Technology plays its part by continuing to develop, implement and market strong technical solutions. Employers who choose to implement family friendly policies encourage the development of strong family values in the home. Access providers can help by not offering clearly illegal newsgroups and by cooperating fully with law enforcement agencies.

Government and law enforcement can help greatly by enforcing existing laws and by appropriately extending laws governing the physical world to the Internet. It would be clearly illegal for someone to launch a cable television network called 'The Bestiality Channel' yet web sites dealing with this subject abound and are easily accessible. Lack of aggressive enforcement as well as loopholes in existing laws means that the public and technology sectors are currently shouldering much of the burden of protecting kids in the online environment.

Rather than creating the Internet equivalent of televisions V-Chip, FamilyClick would like to see filtering services, such as ours, made available to all users by all access providers. An Internet rating system, which would depend on voluntary compliance by all Internet content providers, simply would not work. Education and awareness along with cheap and easy access to an effective filter, as well as the right not to use a filter, ensures that parents can make the final determination as to the best method of delivering the enriching content of the Internet to their families.

Thank you for giving me the opportunity to discuss this important matter with you today. FamilyClick looks forward to continuing to work with the commission on this issue and I will gladly answer any questions you may have.

Appendix A - FamilyClick Access Levels and Content Categories

July 20, 2000

	Full FamilyClick Access	**Teen**	**Pre-Teen**	**Kids**	**Children's Playroom** Access to FamilyClick approved sites only
Exclude the following categories					
Crime	X	X	X	X	
Hate Groups	X	X	X	X	
Pornography	X	X	X	X	
Illegal Promotion of non-medical Drugs	X	X	X	X	
Gambling Online	X	X	X	X	
Violence	X	X	X	X	
Chats not DDRTM Protected	X	X	X	X	
Personals		X	X	X	
Illegal Drug Promotion		X	X	X	
Unmonitored Chats		X	X	X	
Non-FamilyClick Email		X	X	X	
Revealing Attire			X	X	
Advanced Sex Education			X	X	
Weapons			X	X	
Games			X	X	
Basic Sex Education				X	

Biography

Sheridan E. Scott

Chief Regulatory Officer

Sheridan Elizabeth Scott is Chief Regulatory Officer of Bell Canada. Ms Scott's responsibilities include maintaining regulatory relationships with the CRTC, the Commissioner of Competition, the Copyright Board and the FCC. She also oversees public policy issues for Bell Canada, Nexxia and ActiMedia, particularly with respect to the Internet and e-commerce. Prior to her appointment on August 1, 1999, Ms Scott was Vice President - Office of the President.

Ms. Scott completed her legal studies at University of Victoria after spending five years at the Canada Council and the Social Science & Humanities Research Council. She returned to Ottawa as Law Clerk to the Chief Justice of Canada, the Rt. Honourable Bora Laskin, and was subsequently called to the Bar of Ontario. In 1983, she joined the legal department of the CRTC where she was involved in major public hearings on long distance competition, the regulation of cable rates, the renewal of pay and specialty licenses and a complete review of all broadcasting regulations. She left the CRTC in 1992 to take up responsibilities as Assistant Vice President, Planning & Corporate Development at the Canadian Broadcasting Corporation (CBC). The following year she was appointed Vice President of Planning and Regulatory Affairs with responsibilities for affiliate relations, regulatory matters, resource planning and audience research.

In 1994, Ms Scott joined Bell Canada as Vice President, Multimedia Law & Regulation. She was responsible for managing the legal and regulatory issues associated with the evolution of the broadband multimedia capacity in Bell's network and in its operating activities.

Ms Scott is the author of several articles on communications law. She is Chair of the Board of Directors of Canadian Women in Communications (CWC); Founding member, National Capital Association of Communications Lawyers (NCACL); Director of Opera Lyra Ottawa; Director and Vice-Chair of the Bell Broadcast and New Media Fund as well as a member of the Ontario Digital Media Growth Fund. She recently joined the Board of the Internet Content Rating Association (ICRA).

Ms Scott and her husband David Zussman, live in Ottawa with their two children Richard and Julianne.

COPA Commission Hearing II

Testimony given by Sheridan Scott, Bell Canada, Board Member, Internet Content Rating Association

Introduction

Thank you, Chairman, for this opportunity to testify to this hearing of the COPA Commission. My name is Sheridan Scott and I am the Chief Regulatory Officer for Bell Canada and I am a Board member of the Internet Content Rating Association (ICRA).

Background on ICRA

ICRA is unique in the field of labelling and filtering. We are the only non-profit organization operating in this space. Further, we offer a self-rating or labelling service to content providers at our web site, www.icra.org and a filtering service to parents that is embedded in two of the major browsers, Microsoft's Internet Explorer and Netscape's Navigator. Both of these services are free of charge. Our costs are met through a mixture of membership fees – currently $25,000/year – advertising and licensing fees to third parties. Our eighteen members include many of the best known companies in the Internet sector, for example, Microsoft, IBM, AOL, Novell, Network Solutions, British Telecom and, of course, Bell Canada.

Our dual mission is to protect children from potentially harmful material while also protecting the free speech rights of content providers. Our system is voluntary – we do not seek government-mandated use of the system by content providers – instead we continue to work with the industry to create positive incentives to rate. To date over 150,000 sites have rated using our system and that figure increases by 4,000 sites a month. And with our efforts to internationalize the system, we believe that the number of sites rated will grow exponentially over the coming months and years.

ICRA owns and operates the RSACi rating system. The organization RSAC formally folded into the newly established Internet Content Rating Association in the spring of 1999. ICRA has offices in the US and the UK and has recently been awarded a grant from the European Union for $650,000. The grant covers a number of work areas including: to expand the number of categories of the current system, to translate the rating questionnaire into at lease five major languages, and to launch a major marketing and promotion campaign directed at both content providers and the general public – raising awareness of the system with ordinary parents.

How RSACi works

I'd like to speak briefly about how the current RSACi system works. Firstly, a content provider comes to our site and fills in a content questionnaire which asks the applicant about the portrayal of content on their site under four categories: Nudity, Sex, Language and Violence. As the applicant fills out the online form, a rating level is recorded in each of the four categories and is converted into an html meta tag written in the PICS language. After the content provider has finished the questionnaire, they must agree to the ICRA Terms and Conditions, which include a statement that they have not wilfully misrepresented themselves.

At the completion of this process, the meta tag is displayed on the screen and instructions given on how to copy and paste it into the header of their home page and that label will cover the content for their entire site. They can, if they wish, label individual directories, pages or even images separately. Many sites also place the "We rated with RSACi" logo on their home page or, increasingly, the words, Content Policy next to their Privacy Policy.

The parent or concerned adult uses the filtering system in a very different way. They activate the parental controls within their browser and set the levels they feel are appropriate for their children. They use the Content Advisor controls within Internet Explorer and NetWatch within Navigator. After inputting a password, they can choose what levels of Nudity, Sex, Language and Violence they feel is appropriate for their child. In addition, they can choose to select the Do Not Go To Unrated Sites function. Should access to a site be blocked, the system explains why, gives the rating for the site and even allows the parent to override the blocking with a password. Further, a blocked site can be added to an Approved site list so that the child can access the site in future whether or not it is rated.

The revised system

From the launch of the RSACi system in April 1996, content providers from around the world have used our self-labelling system. They have done so in spite of the fact that the questionnaire is written in American English and reflects a US-centric view of the world. In 1998, RSACi won the prestigious Carl Bertelsmann Prize from the Bertelsmann Foundation in Germany for recognition of outstanding innovation in the area of self-regulation on the Internet. The Foundation, together with our existing North American members and a number of key European and Japanese companies and associations, not only formed the international organization, ICRA, but have also worked on a revised system due to be launched in October of this year. Here is a summary of the new elements of this system:

- A new labelling vocabulary with detailed, objective descriptors
- New categories of concern, including: intolerance, alcohol, drug and tobacco use; the ability to block chat rooms and the introduction of Context in the questionnaire
- Filtering "templates" allowing parents to choose a familiar rating system, e.g., a movie rating system, which is mapped back to the ICRA labels
- The inclusion of black and white lists of acceptable or non-acceptable sites
- The system translated into at least five major languages of the world

- Greater simplicity of use for both content providers and parents

The final details of the system are still being finalized. Suffice it is to say that the views and comments, complaints and criticisms of many hundreds of our users, an international advisory board, a European consultative group and many from the press and media have helped us to form our revised system. There are plans to develop an ICRA search engine, to license the growing database of rated sites and to offer the revised system to other third parties around the world interested in using the questionnaire for rating traditional media, such as television, film and other converging media.

Monitoring, checking and auditing

Alongside our developments of the rating system is our continued commitment to ensure that the system is not abused and that those attempting to cheat it are identified and dealt with. We use a number of methods to monitor and check up on sites including:

- An automated web crawler that checks the ratings in our database against the meta tags in a site's header
- Spot checking of sites on a daily basis, particularly sites with provocative URL names
- Responding to users complaints or reports on sites they feel have mis-labelled

Web masters must accept our Terms and Conditions of Use if they are to use our meta-tags. In the very rare number of instances where mis-labelling has occurred, we have contacted the site and they have either re-labelled their site or taken the label off altogether. As the number of sites increases and the job of auditing expands, we plan to utilize a neutral third party to take on this important monitoring work.

Achieving critical mass

For ICRA, or any self-labelling content system, to succeed, there must be a critical mass of users labelling their sites and parents filtering web sites they don't want their kids to see. To achieve this, ICRA has identified three critical markets:

- Adult-only sites
- Children-oriented sites
- The Top 1000 sites

The early adoption of the existing RSACi system by adult entertainment sites is very encouraging. Playboy.com was one of the first sites to rate and 15% of all the RSACi rated sites are in what would be considered the pornographic category. Children sites are another top priority. Disney was an early supporter and ensured their sites were labelled. And the Top 1000 sites are of major importance, as they account for 80% of the traffic on the web.

For the ICRA system to become an integral part of the Internet landscape, public awareness campaigns must be launched and sustained in North America and throughout the world. Parents need to know that there are ways to protect their children online. One of the greatest inhibitors to the growth of the Internet is fear – parental fear of what their children will see and experience on the net. We hope that the ICRA system proves to be a very useful tool in the toolbox of programmes and applications that can help parents to overcome their fears and bring their children the extraordinary benefits of being online.

Positive incentives to rate

I stated earlier that the ICRA system is a voluntary one. We do not seek, nor would we want the COPA Commission to propose to the US or any government that there should be a legislated mandate to use the system. Instead, we wish to work with the Internet community to develop ways to encourage content providers to rate and for parents to filter without resorting to laws. Here are a few examples of existing and proposed incentives:

- The "do not go to unrated sites" option in the browser
- Sites that will only link to other rated sites (e.g., Disney)
- Search engines and hosting services that encourage their registered sites to rate
- Incorporation of the ICRA system in web authoring tools (e.g., FrontPage)
- Development of an ICRA search engine
- Providing legal protection from prosecution if an adult site is rated (as in Germany)

The US government has an important role to play in encouraging the concept and practise of self-regulation to flourish and grow. We sincerely hope that the COPA Commission will stress the need for government support and backing to our efforts and those of the parental filtering movement. While we oppose any government requirement to label a site, we would be keen to explore using existing or proposed legislation that backs up the use of the system – particularly as a defence against prosecution or as part of a co-regulatory regime.

Further, we can only stress the essential element of international co-operation and joint initiatives on this, the most multi-cultural of all media. Indeed, this Commission may wish to review and take into account a wide number of government/industry initiatives that have emerged in Canada, in Europe, in Australia and in Japan. Protection of children is a global pre-occupation and countries around the world are now focused on the need for internationally acceptable ways to deal with a range of difficult issues, including the means to protect children from material that is easily accessed, downloaded and distributed off the Internet. We wish you well in your deliberations.

Joseph Field, Co-Founder/CTO
Pearl Software

Mr. Field has a background in electronic hardware and software development. Joe received his undergraduate and MSEE degree from the University of Delaware where he also continued post-Masters work toward a Doctorate. His area of research centered around high speed networking. Joe was also involved in the early days of the ARPANET, which has evolved into the Internet of today. Joe's professional career has found him playing a leading technical and management role in developing numerous commercial products, including industrial control products and systems, computer workstations and industrial data monitoring equipment.

Joe's expertise in data monitoring systems combined with his passion for networking topologies and protocols has elevated him to a respected resource on issues centered around Internet communications and information architecture. Joe is an active participant in various technical forums and maintains the technological vision for Pearl Software.

Pearl Software's Testimony to Commission on Online Child Protection

Joseph I. Field, Jr.

Thursday, July 20

Pearl Software is pleased to have the opportunity to speak today about our experiences in protecting children that access the Internet. Since our beginning in 1995, we have approached this problem from that of a parent's perspective. It is generally agreed that we would like to keep our children away from influences that we, as parents and educators, consider inappropriate. At the same time, we do not want to stop our children from learning and exploring the vast, rich, educational resources that are available to them on the Internet. It is our opinion as well as our experience that an approach that combines technology with traditional parental supervision is the most viable way to instill our community and individual values upon our children while simultaneously protecting their on-line well being and privacy. This mix of supervision and technology is mirrored in Pearl Software's products and processes. Our approach of providing a tool that allows parents and educators to monitor online activity has gained wide acceptance and has been showcased at the Internet Summit as well as supported by Louis Freeh, Director of the FBI, and Bill Gates, Chairman of Microsoft Corporation. The issue with relying solely upon a technological approach to protecting children is that most solutions try to solve the problem by definitively or heuristically identifying inappropriate content and subsequently blocking the identified content. Inappropriate content is defined as that which is "unsuitable or improper". "Unsuitable or improper" content is subjective and varies in time, by culture, by geographic region and by age group.

How do we insure the parental prerogative of raising children in an age of online communications? From a parent's perspective, as our environment changes and as issues change, so must we change in our approach to protecting our children and imparting upon them behaviors that we, as caregivers in collective communities deem appropriate. When our children are young, we watch them closely while in public places or dangerous situations and we reprimand inappropriate behavior in order to alter or prevent future occurrences of that behavior. It is this traditional approach to parenting and educating that must not be lost in the equation when formatting a solution to protect children while online. This concept has been incorporated into Pearl Software's technological solution to protecting the safety and privacy of our children.

Experience and our customers tell us that parents and educators desire a technological tool that compliments their efforts in attempting to raise responsible children. Pearl Software's Cyber Snoop is a comprehensive software package that gives parents and teachers the ability to chaperone and control their children's on-line activity as well as protect their children's privacy. Cyber Snoop was developed with the philosophy that while we trust our children, we must have a means to supervise and guide them. Just as we watch our children in public places or dangerous situations, our product's monitoring component keeps track of Internet places visited and information exchanged. If questionable Web locations are found, the parent or educator can use this monitoring tool to quick-link to that site and immediately view its content. If questionable e-mail, news, or chat activity is found, the content of these messages is easily viewed in the same manner. This technology can also be configured to selectively or completely restrict Internet access or provide no monitoring capability at all. Thus, the level of supervision is easily configured to an individual's needs and the definition of inappropriate behavior is left to the discretion of the parent or educator. This technological solution removes government censorship and First Amendment issues and replaces them with issues of parenting and educating our children.

At Pearl Software, we believe all segments of the Internet need to be addressed when considering our children's well being. The media, public discourse, and filtering solutions have placed an unbalanced emphasis on pornography that is accessible through the World Wide Web. While we agree that this segment of the Internet can pose a direct threat to our children's innocence, we consider the interactive Internet mediums to be an equal, if not greater, threat to our children's well being. Specifically, chat rooms, instant messages, news postings and e-mail expose our children not only to mental danger, but potential real physical danger. To protect our children in these interactive mediums we believe there is no substitute for parental vigilance and supervision. While a child may communicate and strike up a friendship with an open attitude, with a monitoring tool in hand, a parent may view the same interaction in a more cautious light. By providing parents and educators with insight into the child's activity, the caregiver can intercede before a seemingly innocent exchange of information and conversation escalates to a physical meeting that may have irreversible consequences.

Our technical approach in providing the Cyber Snoop solution has encompassed many design considerations. One such consideration was the usefulness of supporting a list of URLs considered inappropriate. In essence, creating a URL filter. As stated earlier, inappropriate content is subjective. As such, parents and teachers would be forced to rely upon the judgment of Pearl Software to determine what is and what is not appropriate material. We consider this to be a losing battle for two reasons: 1. The World Wide Web Internet medium continues to grow at geometric rates and 2. as humans, we are fallible and that fallibility would ultimately manifest itself in any filtering solution. One of the Internet's most comprehensive search engines, Alta Vista, has less than 16% of the existing Web pages cataloged[1]. How can a company the size of Pearl Software, or its competitors, categorized 100% of the web pages that exist? It can't and to portend otherwise would be selling our customers a false sense of security. In designing Cyber Snoop we opted to place control in the Parent's and Educator's hands by supplying control mechanisms that protect the dissemination of personal information, allow time restrictions, and allow access to individually defined allowable subsets of each Internet medium.

Another design decision that Pearl Software incorporated into Cyber Snoop is the control of Internet content based on rating system standards. Cyber Snoop supports the PICs rating system, which relies on content providers voluntarily rating the content they create and distribute. On Web pages, information exists in the header (hidden part) of the Web page that contains the rating code for that page. Cyber Snoop looks at the page rating code and compares it to the levels the parent or educator specifies as acceptable.

---

[1] Lawrence, S. & Giles, C.L., Nature 400, 107-109 (1999)

There are various rating systems that have been developed and are currently being used on the Internet. PICs rating systems attempt to characterize the nature of Web pages and other Internet content. Parents and Educators can use Cyber Snoop to define acceptable rating levels for each rating system available. Cyber Snoop can be set to monitor multiple rating systems simultaneously and can also be set to block any content that is not rated. The incorporation of a secure rating system control into Cyber Snoop was done because we believe this approach bolsters a caregiver's ability to determine what level of content a child has access to. The down side of this approach is that this rating system relies on content providers voluntarily rating the content they create and distribute. Though a small margin of error may be acceptable, a rating validation mechanism must be implemented to fully effectuate using rating systems on the Internet.

Throughout the past half decade, the Internet has grown quickly across borders and cultures. The Internet is too large and too dynamic to control with a broad legislative brush. In fact it is antithetical to our history and our current way of life to stifle the progression to a future that provides greater access to information and expression of freedoms. Instead our approach to ensure our collective well being in this new world of information access must continue to rely upon traditional parental values and methods that have proven effective throughout time combined with new tools and techniques that bolster and complement these values and methods.

Contact Information:
Pearl Software, Inc.
64 E. Uwchlan Avenue
Suite 230
Exton, PA 19341
(610) 458-2387
www.PearlSoftware.com
information@pearlsoftware.com

© 2000 Pearl Software, Inc.

Select Relationships and Initiatives:

Pearl Software Education Foundation

The Pearl Software Education Foundation is a not for profit entity that provides educational resources and safety programs to the growing Internet user community. The Foundation strives to help the Internet proliferate as an educational medium while providing a means to protect the safety of those accessing it. The Foundation's emphasis is placed on responsible Internet usage that can only be achieved through education. Pearl Software, Inc. is a primary contributor to the Foundation.

EarthLink Internet

EarthLink Internet has selected Cyber Snoop for inclusion on EarthLink's TotalAccess™ and EarthLink 5.0 Internet access software CD-ROMs. EarthLink has taken a proactive step toward ensuring the safety and well being of its members by providing them with tools that enhance their Internet use and make it more productive and enjoyable. This partnership will market approximately 15 million copies of Cyber Snoop to EarthLink's target audience.

Disney & General Mills

Pearl Software has teamed with General Mills and Disney Interactive to distribute a promotional CD-ROM sampler disc. Upon purchasing selected General Mills' cereals, parents will have access to interactive CD-ROM games, limited free Internet access and Pearl Software's Cyber Snoop. This partnership will market approximately 5 million copies of Cyber Snoop to General Mills and Disney's target audience.

Compaq Computer Corporation

Cyber Snoop software has been chosen for inclusion in selected Compaq Computer Corporation LearningPaq educational solutions. Compaq's LearningPaq provides educators with tools that enrich a child's educational experience and understanding of technology.

Ray Soular
Chairman
SafeSurf

Ray Soular has been involved in the computer industry since 1981. His software innovations earned him the Golden Disk Award for programming excellence at the 1983 Consumer Electronics Show and a rating of "11" on a ten point scale by Electronic Musician Magazine. Ray Soular was involved in the evolution of the Music Instrument Digital Interface (MIDI) Standard and designed the first CD ROM vending machine.

His desire to insure that children would safely benefit from the Internet's knowledge explosion lead him to form SafeSurf in 1995 and to serve on the technical committee developing the PICS protocol. Ray Soular was listed as among the 100 most influential people on the Internet by Website Magazine in 1997 and nominated for the 1999 World Technology Award for Ethics.

Testimony of Ray Soular
Chairman of SafeSurf
Before the Commission on Online Child Protection
Hearing on July 20, 2000

I thank you for inviting me to speak before people who have dedicated themselves to protecting children online. When I received my invitation to speak here today, I was impressed by one particular sentence in which Donald Telage wrote that the Commission is "more interested in your insights into the characteristics of particular technologies or methods that cause them to be adopted (or not), to be effective (or not), and that bear on pertinent legal and policy concerns." It is to this directive that I speak. I will not focus this discussion on technology, but on why that rating technology has not been adopted into wide spread use.

Before we can examine where the concept of online rating has faltered, let us retrace the events that have lead us to our present situation. Rating online content only existed as a concept in academic white papers until May of 1995, when SafeSurf implemented the first rating system designed to protect children on the Internet. It consisted of placing in the HTML code, an identifier known as the SafeSurf Wave SS~~, followed by a series of numbers that would be interpreted by filtering software. SafeSurf began encouraging Web sites to join a rated online community it called a "cyber-playground", as well as assisting filtering software companies in updating their software to support Internet rating. (See http://www.safesurf.org/ssplan.htm for a further understanding of the SafeSurf Rating Standard.)

By the time, PICS (Platform for Internet Content Selection) Consortium was first convened in late August '95 and before it began it work, SafeSurf had obtained commitments from most of the major filtering companies and formed a rated community of thousands of sites. As a result, SafeSurf was invited to become a member of the PICS Consortium and participate in creating the PICS specification.

PICS represented a broader view in its ability for multiple rating systems and ideas to coexist and thrive, thus preventing any single powerful entity from forcing its rating system on the people. The PICS specification also supports rating to be done by groups using rating servers, provides a rule set, known as PICSRules, to give individuals the ability to communicate their own preferences to search engines and servers, and has been adapted for use in XML and RDF. (See http://www.w3.org/PICS/ for a further understanding of the technology.)

Things were going great; SafeSurf welcomed with open arms the second rating system to convert to the PICS protocol, RASC and encouraged Arthur Pober to propose PICS to Entertainment Software Rating Board. Microsoft had taken the initiative and was preparing to release the first PICS compatible browser. Scott Berkun of Microsoft first preposed the idea of a ratings file so that it would be easier to incorporate more than one rating system in Internet Explorer. Both RSACi and SafeSurf were asked to prepare ratings file and help alpha test their implementation in the upcoming browser.

I'm sure that when God looked down on the PICS protocol and its potential, he saw that it was good, but something was brewing behind the scenes that would change everything and leave a bad taste in the mouth of many Internet communities.

When IE 3.0 was released, Microsoft removed the ratings file of all other systems and decided to include only a single system of its choice. I have no idea where executives at Microsoft derived this single rating system stance, but the choice was not based upon number of sites rated, since SafeSurf had twice as many sites rated at that time as the selected system. Microsoft's decision to hinder diversity was also not supported by the PICS Statement on the Intent, which reads:

"The Web, through PICS implementations, ought to support access to a variety of labeling systems that reflect the diversity of moral and cultural values held by those that use the Net. No single rating system and service can perfectly meet the needs of all the communities on the web."

This move rendered the IE browser implementation confusing and useless, since it could not immediately understand and load over 50% of the rated sites. Microsoft further limited it NT 4.0 Web server to support only a single rating system with it auto-rating feature. The complaints poured in as more and more people became disillusioned about the promise of PICS.

The online community that had had been built with the expectation of diversity was being torn down by a major player using its position in the browser market to push a single rating system on its users. It should be noted that year and a half later, Netscape released its PICS implementation without limiting its browser to a single rating system, but it was a minor victory since Internet Explorer controlled the market.

The lesson we learn from this history is that in order to encourage the cyber-world to adopt online rating, we must recognize and support their desire for enough diversity to choose a system that works for them. If we build our online communities with understanding and cooperation, they will grow faster than the lilies of the field. However, should we attempt to force single minded solutions upon the masses, we will continue to be frustrated by the freedom of the Internet.

Arthur I. Pober, Ed. D.

Dr. Pober is Executive Director of the Entertainment Software Rating Board (ESRB). The ESRB is the rating board established by the Interactive Digital Software Association (IDSA) to provide parents and other consumers information necessary to make informed purchases of interactive entertainment software.

Prior to establishing the ESRB, Dr. Pober was Vice President and Director of the Children's Advertising Review Unit (CARU, the self regulatory arm of the children's advertising industry), for the Council for Better Business Bureaus. CARU was established in I974 to promote truthful and accurate advertising, which is targeted at children.

Dr. Pober has enjoyed a long career in the field of education, having held positions such as Principal of Hunter College Elementary School, Director of Special Programs for the Board of Education for the City of New York, and Director of Gifted and Talented Education for New York City among others.

He has worked extensively in the public and private sectors to create and develop programs and learning materials for children, and has lectured throughout the world on topics ranging from education, intelligence training and arts education. He currently serves on the advisory boards of the Jewish Museum, Child Magazine and the new ABC television show "Science Court".

He received his doctorate in Educational Psychology and Organizational Development from Yeshiva University.

TESTIMONY OF DR. ARTHUR POBER
PRESIDENT OF
THE ENTERTAINMENT SOFTWARE RATING BOARD
BEFORE THE COMMISSION ON CHILD ONLINE PROTECTION
July 20, 2000

Good afternoon, Mr. Chairman, and thank you for the opportunity to appear before your commission as it examines technologies and methods that may reduce online access by minors to harmful materials within the meaning of the Child Online Protection Act ("COPA"). My name is Dr. Arthur Pober and I am President of the Entertainment Software Rating Board ("ESRB"). Prior to establishing the ESRB, I was the Vice President and Director of the Children's Advertising Review Unit ("CARU"), the self-regulatory arm of the Council for Better Business Bureaus. I am also an educator and served as principal of the Hunter College Elementary School as well as Director of Special Projects for 26 elementary, and 11 intermediate schools in New York City. Today I will be speaking specifically about ESRB's online rating and labeling methods, as that is my area of expertise. It is an honor to testify before you today.

The ESRB is an independent, self-regulatory entity that provides comprehensive support services to companies in the interactive entertainment industry. Established in 1994, the ESRB is the nation's leading non-profit, entertainment software rating body. Although originally charged with developing a standardized rating system for entertainment software, since its inception the organization has grown proactively in protecting consumers and anticipating the evolving industry. Today – after rating over 6,500 game titles and having been praised by Senator Joe Lieberman as the "most comprehensive rating system of any entertainment medium in this country" – the ESRB has evolved into a dynamic and effective self-regulatory organization. This organization has established itself as one of the preeminent institutional models for effective and meaningful self-regulation for interactive entertainment. We now provide services not only for rating software titles, but also for rating websites and online games, for ensuring online privacy protection, and for reviewing advertising created by the interactive entertainment industry.

ESRB Interactive ("ESRBi") is the division within the ESRB that provides the ratings for websites and online games in conjunction with online oversight and enforcement mechanisms. The mission of ESRBi is to provide parents, web consumers, and the online community-at-large, with objective information that facilitates informed decisions regarding Internet use and online content. ESRBi issues ratings that provide information on the age appropriateness of a site and information on the site's content. It is the only interactive entertainment rating service that does both. There is no cost to the consumer. Publishers pay a nominal fee to obtain ratings for sites.

ESRBi does not in any way restrict access to games or websites. Like other effective and meaningful rating mechanisms, the ESRB operates independently to realize its goal of affording objective information, rather than dictating taste or censoring content. The ESRB and ESRBi ratings are designed to give consumers information about the content of an interactive video, website, online game, or computer entertainment title and for which ages it is appropriate. Our goal is to provide information to consumers so that they can apply their own values, experiences, and standards to determine what kind of interactive entertainment is and is not appropriate for their home. Choices about interactive entertainment should be no different than the choices made about films, music, TV shows, and books. To make the system work best for the consumer, the ESRB has invested significant time and money into numerous educational initiatives, public relations campaigns, and also maintains a website (www.esrb.org) and a toll-free line (800-771-ESRB), where consumers can get the most current ratings for each product we have rated. Currently, our site receives an average of one-million hits per month, and our toll free line averages over one-thousand calls per day.

How ESRBi Works

Interactive ratings are generated by raters, randomly selected from a demographically diverse pool, who independently review the submitted materials and the site and generate a consensus rating based on ESRBi rating criteria. ESRBi raters have no ties to the interactive entertainment industry and are trained intensively in evaluating interactive entertainment content. After an interactive rating has been issued the site is monitored periodically to ensure that the constant areas remain unchanged and/or that the rating is accurate.

If an entire website is rated, the ESRBi symbol is located on the home page of the site. If only a section of the website is rated, the symbol will appear on the first page of the rated web page section. If an online game or interactive arena is rated, the symbol will appear where the arena or game is accessed. There are five rating symbol categories:

- Early Childhood Interactive (ECi) – content may be suitable for ages 3 and older.
- Everyone Interactive (Ei) – content may be suitable for ages 6 and older.
- Teen Interactive (Ti) – content may be suitable for ages 13 and older.
- Mature Interactive (Mi) – content may be suitable for ages 17 and older.
- Adults Only Interactive (Ai) – content suitable only for adults.

The "i" represents websites that contain chat rooms, bulletin boards, multi-player games and/or any space that can provide open forums or interactive exchanges that result in an ever-changing environment on the Internet. Any person who is about to participate in this kind of fluid site is cautioned by the symbol "i" to be aware that the user can exchange information with other users who may have differing and/or controversial opinions, or who may influence game play.

Content descriptors, located on the rating icon, give consumers more detailed information about the product in terms of violence, sexual themes, language, and other areas that may be of interest or concern. If there is no content descriptor, the Rating Board believes that the product does not include content that should be highlighted.

ESRBi issues ratings in two areas on the Internet:

1. Contained Areas receive the traditional ESRB ratings. These areas, known as *Finite Space Arenas*, are websites that allow no interaction between website and user. These would also include sites where users can leave messages, comments or e-mails, but there is no exchange of content or other information that could influence suitability of use. In addition, such sites do not allow users to advance to a more controversial or sophisticated level.

2. Interactive Sites receive the ESRBi icons. These areas, known as *Free Space Arenas*, provide opportunities for users to engage in an interactive experience. These may take the form of an entertainment site (i.e., game) with another interactive option (i.e., bulletin boards, chat rooms, additional participants). Sites where users can influence or create content are classified as interactive and represent a *Free Space Zone* where there is less control.

Following is a step-by-step overview of the ESRBi rating process:

1. Application is submitted with either the website address, videotape of game-play, interactive software or printout of the website.
2. ESRBi reviews the application.
3. Three raters evaluate the content.
4. The raters issue a rating based on a consensus of at least two raters.

5a. An interactive rating with content descriptors is issued.

5b. If the publisher accepts the rating and descriptors, the submitting party signs the rating certificate.

5c. If the publisher does not accept the rating and descriptors, the publisher may edit and/or adjust the content and resubmit the website. Upon resubmission, steps 3 – 5 are repeated.

Oversight and Enforcement

Companies participating in the ESRBi rating program agree to the same Terms and Conditions letter used for ratings on packaged goods. Submitters are informed that inaccurate representations may result in the imposition of penalties, including but not limited to, the revocation of a rating, issuance of a new rating and/or the commencement of litigation. Additionally, companies are required to notify ESRBi upon making any major modifications to the content of the website.

In addition to the notice requirement, interactive and online game sites are reevaluated at least four times a year by a monitor. Each monitor is specially trained and randomly views online game sites to ensure that the companies are properly posting the rating icon. Failure to comply with ESRBi requirements may result in the imposition of penalties, including but not limited to, the revocation of a rating, issuance of a new rating and/or the commencement of litigation.

America Online Initiative

ESRBi is committed to increasing the public's awareness and understanding of the interactive rating system. We are committed to informing web users of their choice regarding what kinds of websites and interactive entertainment they and their children are exposed to. In an effort to fulfill this commitment, ESRBi has joined forces with America Online ("AOL"), the world's largest online service.

AOL now requires all games played on its service to be rated by ESRBi, and will work with others in the interactive entertainment industry to push for widespread adoption of game ratings throughout the Internet. Games rated Adults Only or not rated at all will not be available on the AOL service. AOL also requires their commerce partners, such as eToys.com and Beyond.com, to prominently display the ESRBi ratings. Additionally, AOL and AOL.com have each established an online education area with information for consumers about this new policy, including a link to the ESRB website as well as other helpful resources for parents. AOL is also developing new Parental Control functions that will let parents block their children's access to any or all games on AOL based on the ESRBi ratings.

To make our alliance with AOL most effective, ESRBi and AOL have formed a task force focused on obtaining broad support for industry-wide adoption of ratings for all online games, demos, and games editorial sites. The task force is comprised of members of the academic, business, retail (both online and traditional), governmental, and media communities. This task force will meet periodically to discuss and facilitate its mission.

Online retailers such as Blockbuster.com, Amazon.com, GameDealer.com, and ElectronicBoutique.com also carry the ESRB ratings.

ESRBi is pleased to receive support from a major entity like AOL, and we look forward to creating more alliances with other online services.

What is the relevance of traditional labeling or rating of movies, music, TV shows and video games to the Internet?

Based on consumer research done by the ESRB, we found that the traditional labeling seen on movies, music, TV shows and video games is the most easily understood and common mechanism of product information relied on by consumers. Because consumers already trust and rely on the information contained in traditional labeling, using a variation of this system such as the ESRBi rating icons and descriptors on the Internet is the best way to inform web users about the content of certain websites and online games.

What information is available regarding parents' awareness and attitudes about Internet filtering, rating/labeling?

ESRB furthers its commitment to consumer education by distributing information about the rating system through brochures, pamphlets, print ads, retailer outreach, organizational partnerships, public relations campaigns and public service announcements.

What legislation would be most appropriate to promote awareness and effective use of filtering, rating or labeling systems?

The most important factor in promoting awareness and increasing effectiveness of rating and labeling systems is education. For example, 35 years ago the MPAA implemented the independent and effective rating system consumers rely on today. Governmental intervention was not necessary because the MPAA educated and informed consumers and industry leaders as to the importance and relevance of the rating system.

In the six years the ESRB has been in existence we have remained ahead of the curve in implementing a standardized rating system. Consumer research and education has been the foundation upon which the rating system has grown. By sharing information about the labeling system with consumers, retailers, and web publishers we have become a major force in interactive entertainment self-regulation. However, because the global electronic medium is in its nascent stage, education regarding the use of Internet rating systems is still developing. As such, the e-marketplace requires experienced and capable hands to assist it in achieving its fullest potential. The online interactive entertainment industry is highly motivated to adapt quickly to marketplace changes and employ meaningful measures that will protect consumer rights. The people and companies that deal with the industry's constant change and unique requirements are those in the best position to guide and refine its development. As all successful and responsible business people realize, consumer education and protection is an essential element of this development. An online business that cannot assist parents in protecting children from harmful content is a business that will fail.

Government regulation could well obstruct the existing market incentives that have already begun to inspire industry dedication to consumer protection. Furthermore, governmental regulations are jurisdictionally self-limited. In a global electronic marketplace, differing jurisdictions and incompatible regulations will surely generate wasteful conflicts between nations, federal and state governments, and between the states themselves. The result will certainly be the accompanying protracted litigation of choice-of-law statutes, provisions, and agreements.

The government's role should be to encourage and facilitate industry-led self-regulation. To be effective, the online industry requires speed and flexibility to self-regulate the dynamic e-marketplace. By combining adaptability with stability, self-regulatory programs led by industry and nurtured by government provide the most effective protection for consumers in the online arena.

Should government conduct, sponsor or fund research into improving filtering, labeling and rating systems?

The interactive entertainment industry has shown it is capable of researching and implementing ways to improve labeling and rating systems. In the six years the ESRB has been in existence, we have grown in response to changes in technology and consumer need. Today, ESRB provides services not only for rating software titles, but also for rating websites and online games, for ensuring online privacy protection, and most recently, for reviewing advertising created by the interactive entertainment industry. The development of these additional services came as a result of conducting thorough consumer research and having highly trained, experienced employees to implement any necessary changes to improve our methodology.

With the industry already taking on the responsibility of conducting research into improving labeling and rating systems it would be duplicative and fiscally imprudent for the government to sponsor similar research. Furthermore, the private sector is better equipped to interpret the research and implement necessary changes. Failure to do so will result in unhappy consumers thus, a failed business.

Must a filtering, labeling or rating system be international in order to be effective?

For this global medium, an international application is crucial. With the increase in online retail transactions and the advent of online gaming, in order for a labeling or rating system to be meaningful and effective, it must address the lack of international borders within the Internet. ESRB is in the process of doing just that, through various alliances in Canada, Europe, and South America.

What are the implications of filtering and labeling technologies for privacy, first amendment rights and law enforcement?

Sensitivity to issues of privacy and the First Amendment is needed in balancing the interests of consumers and web publishers. At ESRB, we believe we have struck the ideal balance. We do not restrict access to websites or online games. We do not censor or dictate taste. We merely make available effective and meaningful ratings that provide consumers with the necessary information to make an independent decision regarding whether to purchase or participate in an interactive entertainment product.

For example, companies participating in our ESRB Privacy Online program do not collect personal information from children under 13 years old. The ESRB Privacy

Online program combined with the ESRBi rating and monitoring program provide an interactive environment where parents can exercise control by deciding what content their children are exposed to.

Furthermore, participating companies that violate any element of the Privacy or ESRBi programs are subject to the imposition of penalties, including but not limited to, the revocation of a rating and /or the commencement of litigation. The ESRB rating and monitoring system carefully balance the interests of consumers and web publishers while providing for legal remedies in the event of program violations.

How do current labeling and rating systems operate?

Following is a step-by-step overview of the ESRBi rating process:

1. Application is submitted with either the website address, videotape of game-play, interactive software or printout of the website.
2. ESRBi reviews the application.
3. Three raters evaluate the content.
4. The raters issue a rating based on a consensus of at least two raters.

5a. An interactive rating with content descriptors is issued.

5b. If the publisher accepts the rating and descriptors, the submitting party signs the rating certificate.

5c. If the publisher does not accept the rating and descriptors, the publisher may edit and/or adjust the content and resubmit the website. Upon resubmission, steps 3 – 5 are repeated.

Oversight and Enforcement

Companies participating in the ESRBi rating program agree to the same Terms and Conditions letter used for ratings on packaged goods. Submitters are informed that inaccurate representations may result in the imposition of penalties, including but not limited to, the revocation of a rating, issuance of a new rating and/or the commencement of litigation. Additionally, companies are required to notify ESRBi upon making any major modifications to the content of the website.

In addition to the notice requirement, interactive and online game sites are reevaluated at least four times a year by a monitor. If the monitor finds anything inconsistent with the rating, ESRBi automatically changes the rating to reflect the content and sends a letter to the company notifying it of such change. If the company disagrees with the new rating, it may avail itself to the Appeals Board for a final determination. Furthermore, a trained, experienced monitor randomly views the online game sites to ensure that the companies are properly posting the rating icon. Inaccurate representations may result in the imposition of penalties, including but not limited to, the revocation of a rating and/or the commencement of litigation.

What evidence exists regarding the effectiveness of current labeling technologies at restricting access to material that is harmful to minors as defined in COPA?

With the implementation of the AOL initiative, task force, and various retailer initiatives, minors have increasingly less access to age inappropriate information. For example, AOL will not make available on its service games deemed by ESRBi as suitable for adults only, or games not rated at all. Also, AOL is developing new Parental Control functions that will let parents block their children's access to any or all games on AOL based on the ESRBi ratings. Additionally, online retailers such as eToys.com and Beyond.com are enforcing AOL's policy.

AOL is the largest Internet service provider with over 19 million users. The fact that AOL has enough trust and confidence in the ESRBi rating system to create new policies and form a task force dedicated to increasing Internet game ratings is evidence of the effectiveness of the ESRBi rating system.

To what extent if any do such systems also have the effect of restricting access to harmless material of interest to minors?

ESRBi provides ratings in the form of labels on and throughout websites. We do not restrict access to any information. An effective rating system provides information that allows parents to make informed and educated decisions about what material their children have access to and, if they choose to, restrict and filter such information from their children.

How many labeling and rating systems are in the marketplace, and to what extent are websites labeled or rated?

ESRBi has rated 282 websites. Each of these websites may host one or several hundred online games, which are also rated by ESRBi. Additionally, each of these sites may host one or several hundred non-gaming interactive arenas also rated by ESRBi.

What prevents more widespread adoption of rating/labeling by websites and what can be done to further their adoption?

ESRBi needs the same kind of commitment from Internet service providers as it receives from AOL. ESRB became successful through the support of retailers enforcing our ratings and the same kind of support from online retailers is still needed. Our alliance with AOL and its commerce partners sets a precedent for all Internet service providers and online retailers. ESRBi is confident that our relationship with AOL will sharply increase the visibility and overall use of our interactive rating system.

Conclusion

The emergence of the Internet and electronic commerce has brought the issue of online content control to the forefront of the electronic age. In the battle for electronic survival of the fittest, the companies that thrive will be the ones that implement and maintain effective, meaningful measures that assist parents in choosing the appropriate content for their children. We believe that the ESRB Interactive program is the most complete, cost-effective and comprehensive means to achieve that goal. Backed and administered by the experience, expertise and success of established authorities in self-regulation and the Internet, ESRBi provides clarity, support and direction for providing maximum online consumer choice.

I thank the Commission for the opportunity to share these views and discuss these critical issues.

Michael Zimmerman is the News Editor of eWEEK, a weekly magazine and online news site covering the high tech industry. Zimmerman has been with the magazine, a Ziff-Davis Media publication, and covering the industry for 12 years. As a reporter, he broke weekly stories about the movers and shakers of the industry, as well as stories about how technology was being used to improve life. For example, Zimmerman was one of the first to report on IBM's work with the National Center for Missing and Exploited Children and the company's development of age-progression software. In his role as News Editor, which he has been since 1996, Zimmerman has written on a wide range of topics in stories and columns, including a handful pertaining to the starts and stops of the COPA Commission, and the antics of one online pornographer.

Statement to the COPA Commission on ratings and labeling

Presented by Michael R. Zimmerman
News Editor, eWEEK Magazine
July 20, 2000

Chairman Telage, co-chairs, Rice Hughes and Vrandenberg, I would like to thank you for the invitation to participate in today's hearing on rating and labeling technologies. As the first journalist to publish a story about Congress's early missteps with the Children's Online Protection Act of 1998 and how it came dangerously close to missing a year-old deadline to create the Commission in the fall of 1999, I take great joy in being here. And I thank you for the opportunity.

I'm the News Editor of eWEEK Magazine, a weekly publication that covers the hightech industry for the business user of technology In addition to the magazine, which is read by approximately 1.6 million people each week, eWEEK has a very popular Web site, eweek.com, which enjoys about 2 million visitors a week. In my role as News Editor, I direct the coverage of our news team, but also report stories and write a monthly column for our Web site.

What I hope to bring to today's discussion is the online news perspective. From that news perspective, I would argue that a ratings and labeling system, complex as it may be to execute on a global scale, in theory, is undoubtedly a welcome addition to the other tools parents and educators have at their disposal to prevent children from viewing harmful material on the Web. Those other tools, of course, being education and adult supervision. Online news operations, like any other online site, are in a constant battle for eyeballs. We all want visitors, and we all want them to stay.

But we don't want just anybody. Like any other publication, online or print, eWEEK has a target audience. We write for the small businesses and the corporate IT manager/CIO/CEO. Of course, eWEEK online is read by far many more people than just that group. But we maintain our focus in the name of continuity and familiarization. In addition, being true to that audience helps us offer visitors more of what they want.

But not all online sites are as picky about their visitors as news operations. And they'll do just about anything, including deception and trickery, to get people to their site.

In October of 1999 I wrote a story about the near death of the COPA Commission. The story prompted one reader to send me an email about a personal anecdote his child experienced online. It read:

> Mike:
>
> My 12 year old daughter typed in "usmaps.com" while doing research for a school project. The result is what makes me very angry about the internet. There is so much positive benefit the internet brings our society and will bring our kids. There is simply no excuse for anyone, anywhere to try and trick children into viewing pornography.
>
> Thank you for speaking up about the terrible procrastination on this important issue in Washington.
>
> I've got to believe there is technology available that would significantly reduce the possibility of unwanted porn on the net.
>
> Gordon Rogers
> Rocklin, Calif.

What was so horrible about this story is that USMAPS.com was being run by an online pornographer who actually redirected anyone who typed in that URL to his pornography clearing house site, called DIRTBAG.com. To make matters worse, once someone entered DIRTBAG.com, it was impossible to exit without having to shut down the browser. The obvious point, is that this gentleman's daughter was not looking for pornography. She was searching for a map. I submit to you, had the pornographer adhered to a self-regulated rating program or actually been required to rate his site as ``X,'' little real harm could have occurred. (Of course, had the pornographer been required to register his site as .xxx or .sex, none of it would have occurred at all.)

Therein lies what I believe is a major difference between pornography sites and news or other general content sites: like the tobacco industry, unchecked online pornography will try to attract anyone it can, with little or no regard for the unassuming, unknowing, and completely innocent child.

I'm sure you're aware of the University of New Hampshire's recently released report called: Online Victimization: A Report on the Nation's Youth from the school's Crimes Against Children Research Center. The group polled a national sample of 1,501 kids aged from 10 to 17 who use the Internet regularly on a series of topics. Here are some of the results:
Of the 1,501,
19% of the kids had received a sexual solicitation over the Internet in the last year
25% had an unwanted exposure to pictures with sexual content without seeking it
Less than 10% of sexual solicitations and only 3% of unwanted exposure episodes were reported to law enforcement agencies, an ISP, or a hotline
About 40% of those that experienced unwanted exposure to sexual material told a parent
But only about 10% of the parents told could even name a specific authority, like the FBI or CyberTipline, to call in the first place

The report was released June 12.

If eWEEK.com were obligated to adhere to a rating and labeling system, there would be very little, if any objection. Would a ``G''rating stop those who wanted to read eWEEK from doing so? I don't think so. Would a ``G''make someone think twice about drilling into our site? I doubt it. For that matter, I doubt Michael Miller, the Publisher of our sister publication PC Magazine, doesn't object to being placed in the ``technology section''of the local news stand. People who want to read about technology go there.

Those that argue that a measure to create a universal ratings and labeling system would start us down a slippery slope, have a point well worth keeping in mind. It will take contemplative thought and discussion. And of course, it must, be done on an international level.

And there is work being done. As we heard from earlier, the nonprofit Internet Content Rating Association based in the U.K. and U.S. uses the Recreational Software Advisory Council's software-based rating system. One part of the software allows content providers to self-rate and label their sites; while another that's built into browsers such as Microsoft's IE, and filtering software, lets parents set their computers to view only specifically-rated sites. The settings provide parents with an idea about the level of nudity, sex, violence and offensive language that's on a site. The parent can also set the browser to not accept any site that is not RSACi rated. The group, which has a host of big name partners, such as Microsoft, IBM, Bertelsman Foundation, AOL, and the National Science Foundation, is at www.ICRA.org.

Another group, the Internet Content Rating for Europe (INCORE) project, being funded by the European Commission is pushing forward its message of self regulation and self rating of the content originating from and for Europe. And while the primary goal of the Internet Watch Foundation, also of the U.K. is to act as a hotline to which people can report illegal material moving across the Web, it is also offering assistance to ISPs and content providers about rating their sites.

No, these approaches are by no means airtight solutions. Those who really want to bypass filtering can find the way around it, whether it's figuring out the password to unlock the rating/filtering software, or simply going to a friend's house that doesn't use filtering. But rating and labeling is a real and positive step toward curbing children's access to truly harmful material on the Web.

Again, I thank you for the opportunity to participate in this panel.

Dr. Herbert Lin
National Academy of Science

Dr. Herbert Lin is senior scientist and senior staff officer at the Computer Science and Technology Board, National Research Council of the National Academies, where he has been study director of major projects on public policy and information technology. These studies include a 1996 study on national cryptography policy ("Cryptography's Role in Securing the Information Society"), a 1991 study on the future of computer science ("Computing the Future"), and a 1999 study of Defense Department systems for command, control, communications, computing, and intelligence ("Realizing the Potential of C4I: Fundamental Challenges") Prior to his NRC service, he was a professional staff member and staff scientist for the House Armed Services Committee (1986-1990), where his portfolio included defense policy and arms control issues. He also has significant expertise in math and science education. He received his Ph.D. in physics from MIT in 1979. Avocationally, he is a long time folk an

Tools and Strategies for Protecting Kids from Pornography and Their Applicability to Other Inappropriate Internet Content

Computer Science and Telecommunications Board
Board on Children, Youth, and Families
The National Academies

Herb Lin, PhD
202-334-3191
hlin@nas.edu

Michele Kipke, PhD
202-334-3883
mkipke@nas.edu

Summary

The subject of controlling children's Internet access to pornography is charged politically and emotionally in the national debate. Other areas do provoke public concern, but pornography on the Internet is and has been a major focus of national debate for quite some time. Through its primary focus on Internet pornography and threats to children from sexual predators on the Internet, the final report will also, and to a lesser extent, include: (1) an objective description of the risks and benefits of various tools and strategies for addressing pornography that might be used to protect children from inappropriate material on the Internet; (2) an explication of how "packages" of different technological and non-technological tools and strategies can be used together to enable local approaches for protecting children from inappropriate material on the Internet; and (3) case studies of how different communities have approached the problem of protecting children from exposure to pornographic material on the Internet and, again, what those lessons teach about other inappropriate material. Providing a better understanding of different tools and strategies can promote a more reasoned consideration of various public policy options as well as more informed approaches that are locally implementable. The study is expected to provide a foundation for a more coherent and objective local and national debate on the subject of Internet pornography, but will avoid making specific policy recommendations that embed particular social values in this area.

This study originated in a Congressional mandate to the Attorney General by the U.S. Congress in Public Law 105-314 (Protection of Children from Sexual Predators Act of 1998) Title IX, Section 901. The requesting legislation is attached.

Origin

Public Law 105-314 (Protection of Children from Sexual Predators Act of 1998) Title IX, Section 901, mandated that "not later than 90 days after the date of enactment of this Act, the Attorney General shall request that the National Academy of Sciences, acting through its National Research Council, enter into a contract to conduct a study of computer-based technologies and other approaches to the problem of the availability of pornographic material to children on the Internet, in order to develop possible amendments to Federal criminal law and other law enforcement techniques to respond to the problem."

In response to this Congressional mandate, the Computer Science and Telecommunications Board and the Board on Children, Youth, and Families of the National

Research Council (NRC) developed a proposal to convene a committee of experts to explore the pros and cons of different technology options and operational policies needed to support the use of those options. As the result of discussions with the Department of Justice's Office of Juvenile Justice and Delinquency Prevention, the Department of Education, and various private companies in the information technology industry, the study's scope was altered in two ways. The first is that the study now includes non-technological strategies as well as technology options for protection, on the grounds that technology options are one, but only one, element of a comprehensive approach to protection. The second is that the study will be an inquiry that centers on pornography as the primary systematic focus of "inappropriate content", with other areas addressed as appropriate for context-setting purposes, explored incidentally rather than systematically and only as they arise in the context of discussions about specific tools and strategies used in relation to Internet pornography.

Detailed Description

Policy Context

The potential applications of the Internet to enhance and transform K-12 education are well-known today, and many public policy decisions have been taken to provide Internet access for educational purposes. Coupled with the steadily increasing fraction of U.S. classrooms and schools connected to the Internet over the past five years (Note 1), the growing ubiquity of networked information technologies in the home (Note 2) has enabled large numbers of school-age children to reach the Internet. Easy access to the Internet (and related commercial online services) has many advantages for children -- educational materials; online friendships and pen pals; access to subject matter experts; recreation, hobby, sports information; and so on.

At the same time, easy access to the Internet raises many concerns about access of children to inappropriate materials. Of all of the subject areas that might be regarded as inappropriate, pornography is perhaps the area that generates the most pointed societal concern. As a result, there is a reasonably broad social consensus on the undesirability of exposing minors to such material.

Successfully dealing with concerns about pornography and other inappropriate materials is arguably a necessary condition for fully exploiting the educational potential of the Internet. Otherwise, fears about exposure to such material will result in efforts to that may well detract from the positive educational benefits of using the Internet (Note 3).

As a vehicle for understanding the pros and cons of various approaches to protecting kids from inappropriate material on the Internet, pornography is particularly compelling for two reasons. One reason is that, as noted above, pornography is an area that arouses significant concern across a broad cross-section of society. The second reason is that despite this broad social concern about pornography, judgments about what counts as pornographic vary widely. Because the specifics of public concern about pornography thus vary by community, effective approaches to deal with community concerns must account for such variation, and how to account for varying community concerns is a point that is common to dealing with a wide range of material that might be regarded as inappropriate.

The need for parental or teacher involvement in controlling what children can see and read from the Internet is often cited. But as a practical matter, children are likely to have some degree of unsupervised access to the Internet or other online services (e.g., in homes with more permissive parents or simply because of the unfeasibility of continuous parental monitoring of children's Internet use). This reality has led policy-makers to consider various legislative approaches that penalize parties that make pornography available to children and/or require third parties (e.g., content providers, online service providers) to take affirmative steps to restrict the access of minors to such material. Furthermore, this reality has fed public expectations (or at least desires) for a technological solution to the problem (see below).

At issue are three basic problems. The first problem involves a characterization of material, especially images, that minors should not be allowed to view. The law distinguishes between "obscenity" and "indecency", granting a much higher degree of protection to the latter than the former. Pornography per se is not defined legally at all. But whether a given image is obscene (or indecent, for that matter) is difficult to determine objectively. Indeed, it was a Supreme Court Justice who observed that "I can't define it [obscenity], but I know it when I see it." Furthermore, the same image or text can have different meanings and interpretations depending on context. (A recent example is the publication on the Web by the U.S. Congress of the Starr report.)

A second problem is that even if a specific definition of "pornographic" can be stipulated, any technical approach for distinguishing between pornographic and not pornographic material will be imperfect. That is, any means will suffer from both false positives (i.e., material identified as pornographic that a reasonable observer would determine to be not pornographic) and false negatives (i.e., material identified as not pornographic that a reasonable observer would determine to be not pornographic). For example, technical approaches to blocking pornographic material can also result in non-pornographic material being blocked, including artwork, medical images, and the like (false positives), in addition to allowing some fraction of objectionable pornographic material (false negatives). Any plausible and useful methodology for distinguishing between pornographic and non-pornographic must weigh false positives against false negatives and the harm that results from each.

The third problem is that minors must be differentiated from adults if minors are designated as a class of individuals that must be shielded from pornographic or other inappropriate material. It is problematic even when transactions are conducted in a face to face manner. For example, an individual showing a driver's license as proof of age may be showing a falsified license, or may obtain the materials on behalf of an underage friend. In cyberspace, where face to face interactions are not possible, verification of age is much more difficult.

These three problems underscore a key point that is often overlooked in political debates over protecting children on the Internet -- as with all technology, technologies for protecting children on the Internet cannot be viewed as definitive "solutions" in the absence of an appropriate social, cultural, educational, and policy context. Focusing only on the technology to provide protection ignores the potentially larger benefits available from multiple points of control, such as those that might be made available through acceptable use policies in libraries, Internet safety education undertaken in schools, and active involvement from parents.

Technical Context

Technology can provide tools that can help prevent children from accessing on the Internet pornographic and other inappropriate content. Indeed, the legislation requesting this study focuses primarily on technological approaches for controlling electronic transmission of pornographic images. A recent paper (Note 4) notes that decisions on what content can be passed to what recipients are based on three types of information:

- the specific content of the item (e.g., does the item contain a picture of overt sexual activity);
- the recipient's jurisdiction (e.g., is the recipient located in San Francisco, California or in Memphis, Tennessee);

- the recipient's type (e.g., is the recipient an adult or a minor).

The authors of this paper argue further that the architecture of today's Internet denies some or all of the relevant information to any party on whom responsibility might be placed to control access, thus making the imposition of access controls on content particularly difficult.

While technology could facilitate the easier imposition of access controls, the adoption of such controls might well entail other consequences. For example, the imposition of access controls may inhibit technological innovation and increase vulnerability to hardware and software failures. Technologies that facilitate the imposition of access controls would provide a generalized ability to regulate based on jurisdiction and recipient characteristics even for issues beyond content control (to include denial of information to certain recipients based on jurisdiction or type), or provide governments with the ability to regulate access based on the content or the origin of specific pieces of information.

Despite such difficulties, the technical solutions proposed (for either voluntary or mandatory use) generally involve one or more of the four following techniques.

- technically identifying images or text that are potentially inappropriate. For example, if the concern is pornography, text can be scanned for particular words -- an imperfect scan at best, but nevertheless one that might detect some non-trivial fraction of potentially pornographic text. More sophisticated approaches might call for some degree of machine-based understanding of text to identify potentially pornographic material. Pornographic images pose a different problem, because the technology for image understanding and interpretation is still less mature than those for text. A very simple scan of image files for large amounts of flesh tone, for example, is the most basic kind of image recognition technology, but obviously one that can result in a high false positive and false negative rates. More sophisticated techniques employ some combination of features that perform a rudimentary pattern recognition on image files; these techniques are capable of greater selectivity in their identification of potentially pornographic images.
- tagging images or text that are judged to be inappropriate for viewing or access by children, an approach exemplified by the Platform for Internet Content Selection (PICS). Under the PICS approach, content is tagged with a machine-readable label that is generated by the judging party (for example -- is this image pornographic or non-pornographic?). The judging party can be the content provider (whom the PICS approach enables to voluntarily label the content it creates and distributes), or a third party (to whom a parent or teacher can turn to judge the appropriateness of material). (Note 5)
- Identifying sites on which pornography or other material inappropriate for children may be found. This approach depends on a third party judging the appropriateness of a given site for minors; a list of inappropriate sites is then published (and generally integrated into Internet access software that prevents access to those sites).
- restricting access to certain sites (or material) to adults-only. Typically, sites using this approach require the use of a credit card on the assumption that only adults will have access to a valid credit card number.

All of these approaches are imperfect. For example, scanning for flesh tones eliminates historic art and medical information. Tagging content relies on a judgment of a third party that may not comport with the judgment of "pornographic" in any particular situation, and may be much less relevant in the context of user-generated content that may be objectionable. Site-specific approaches deny access to non-pornographic material located on them, and furthermore, sites containing pornographic material emerge daily, so any given list of suspect sites is incomplete by the time it is distributed.

Finally, considerations of how to proceed in the face of technology's imperfections are exacerbated by high rates of technological change. One complication is the fact that a new and better technology is almost always around the corner, leading to (unrealistic) hopes that the next technology will be sufficient in itself provide a perfect (or at least an adequate) solution. A second complication is that policies and procedures that are tied to specific technologies may be rendered obsolete by changes in technology.

It is for these reasons that non-technical dimensions of the problem must be considered.

Social Context

The issues beyond the technological involve those of society, culture, and development. Indeed, the larger context in which technology is embedded involves processes, incentives, laws, and policies have as much -- or more -- impact on the actual protection of children as does technology. For example, what steps do children, parents, schools, libraries, and other institutions need to take when a given technological approach fails to protect a child from pornographic or other inappropriate material or prevents access to desirable content? How do/should parents, schools, libraries, vendors, and other institutions carry out their responsibilities for protecting children from pornographic or other inappropriate material? Such questions are inherently social and cultural.

Furthermore, individuals under the age of 18 -- commonly known as "children" or "minors" -- in fact span a very broad developmental range. What may be developmentally inappropriate for a young child may be more appropriate for a teenager. (For example, a site providing a detailed scientific description of human reproduction may be more appropriate for the latter than the former.) Developmental considerations are thus critical when determining how the Internet may be associated with both risks and opportunities among children and adolescents.

A third social dimension is that the existence of differing philosophies of social control over the definitional process. One philosophy asserts that individual communities have the right (and obligation) to define what is objectionable. A second philosophy, rarely stated but often implicit as the motivating force behind certain policy positions, is the idea that a particular definition of objectionable -- namely one supported by specific advocates with a specific social agenda -- is appropriate for all communities.

Finally, different venues of access must be considered. Controls on exposure to certain types of material that operate in one venue (e.g., school) may be obviated by unrestricted access to all types of material in another venue (e.g., home). Comprehensive restrictions thus require coordinated action among stakeholders that do not always act in such a manner. On the other hand, a choice could be made to allow different degrees of access to objectionable material in different venues (e.g., more restrictive in school, less at home). Either choice might be appropriate depending on the evidence that comprehensive restrictions are needed, the politics of attempting coordinated action, and other non-technical factors.

Plan Of Action

Statement of Task

While a study limited to technology options would help to ensure that public debates over the appropriate approaches to address the problem would be technologically informed, a fully informed debate necessarily goes beyond technology. Thus, while the study will certainly provide a thorough examination of technological options (thus fulfilling the legislative mandate), it will also examine the full range of tools and strategies that can be used to protect children from exposure to pornographic material on the Internet. Many of these tools and strategies may be applicable to other forms of inappropriate material online. The study will focus on tools and strategies for dealing with pornography and then, where appropriate, consider how these same tools and strategies could be used elsewhere. These topics will be addressed in the context of possible options for actions by educators, librarians, parents, industry groups, online service providers, legislators, law enforcement authorities, and policy makers.

To provide a systematic grounding for the analysis, the study will use pornography to illustrate the numerous dimensions of the issue. When appropriate, the discussion of particular tools and strategies will address their utility and applicability for dealing with other types of inappropriate material, though these other areas will not be addressed in a systematic or comprehensive manner. (In other words, other areas will be not be singled out for discussion per se, but rather will be addressed only as they are relevant to discussions of specific tools and strategies.)

For example, one strategy that can be useful as an element of a comprehensive approach for dealing with pornography is the local development, promulgation, and enforcement of acceptable use policies (AUPs). However, any implementation of an AUP must deal with a broad range of issues, only one of which is pornography. The discussion of AUPs would thus illustrate its applicability to other issues that are of concern to various communities, even as it focuses on what might be done about pornography.

This study is not expected to determine what kinds of material should be regarded as pornographic material that is inappropriate for viewing by minors. Instead, it will focus on articulating the various technical, social, and economic risks and benefits of different tools and strategies for protecting children from pornography on the Internet. Furthermore, it will discuss various "packages" of tools and strategies that would be effective for achieving different goals. But because any given goal embeds particular social values, the study will not make specific recommendations for what package should be adopted by the nation. The primary value of this study is to provide neutral, objective analysis of various options so that an informed national debate on the subject can take place.

An obvious question is how this proposal relates to the "GetNetWise" inititative announced on July 29. The answer is that GetNetWise is first and foremost an information resource for those concerned with protecting children on the Internet. That is, it provides information on tools (e.g., specific vendors offering filtering software) and safety tips (e.g., how to conduct yourself on the Internet). However, by design, GetNetWise eschews assessment or evaluation of these various tools.

This proposal takes the next step to explicate the pros and cons of various tools and strategies for protecting children on the Internet, not on a product-by-product or vendor-by-vendor basis, but rather in generic terms (e.g., what are the pros and cons of filtering software). This better understanding of the pros and cons of different approaches to such protection also forms the basis for an analysis of possible policy options at the federal, state, and local levels -- another area avoided by the GetNetWise initiative.

Expertise Required

This project will require perspectives including those of law enforcement, constitutional law, librarians, ethics, and educators, and parents, as well as technical expertise in networking technologies and image recognition. Recognizing the importance of social, cultural, and developmental considerations, the committee will also include individuals with expertise in child and adolescent development, psychology, sociology, and education. Nominations for the study committee will be solicited from a broad range of sources.

Preliminary Work Plan

The National Research Council will assemble a study committee of approximately 12-14 members with expertise in the areas outlined above. The committee will attempt to identify the range of tools and strategies that might be used to protect children from accessing pornography and, secondarily, other inappropriate material on the Internet (Note 6). Furthermore, through briefings, testimony, and public outreach (e.g., public forums in the fact-finding stages), it will seek to understand the risks and benefits of these different options. The committee will attempt to answer questions such as:

- What is the exposure of children to pornography and other inappropriate material on the Internet?
- What technical and non-technical approaches are used today to protect children from pornographic material (as well as other inappropriate material) carried by the Internet and print/film media? (Note 7)
- How does Internet dissemination of pornographic or other inappropriate material differ from the use of other media for such purposes? What are the implications of these differences?
- How effective are known approaches to controlling Internet access to pornography? To what extent are some approaches sensitive to the type of inappropriate material (e.g., pornography vs. hate speech or bomb-making)? How can those approaches be circumvented? What is the ease with which they can be circumvented? What measure of control remains under likely scenarios of circumvention?
- What are some of the current "best practices" used in classrooms and by communities to protect minors from exposure to pornographic or other inappropriate material?
- What are the "false positives" and "false negatives" associated with the technical approaches available today? What is their significance?
- What research is needed to develop new technical approaches and/or social strategies to protecting children from pornographic materials on the Internet?
- What is the social and economic impact of different technical approaches and/or social strategies to protecting children from pornographic materials on the Internet?
- How do the necessary tools and strategies change when pornographic materials are pushed onto children (as opposed to children seeking out pornographic materials on their own)?
- What are possible standards by which to judge the adequacy of different approaches? Can controls on Internet access to pornographic material be as "effective" (however that term is defined) as those for access through other media?
- What are some of the non-technological strategies that might be used by educators, librarians, parents, and local communities to protect children from exposure to pornographic materials on the Internet?

Note: for purposes of this study, it is important to draw a distinction between “operational policy” and “social” or “national” policy. Operational policy issues are narrow in focus and may be required to support any regime of technical controls other than pure “laissez-faire”; operational policy may refer to legislation, regulations, voluntary industry action, or consumer-level actions that relate to technical controls (e.g., technical controls of type X are mandated as an integral element of all computers sold in the U.S.). By contrast, social/national policy issues refer more broadly to issues such as what kinds of material are allowed to circulate on the

Internet and what is the social balance between the value of access to the Internet vs. the harm of access to pornography. Recognizing that operational policy and social policy are not always clearly separable, the study will endeavor to stay away from social/national policy questions on the grounds that it is inappropriate for this study to be involved in making judgments about what kinds of material are or are not acceptable for children to view.

The committee will convene in 7 meetings during the course of the study to solicit input from outside parties, deliberate over its findings and recommendations, and prepare its final report. The budget provides for extensive input to be sought from a wide range of public interest groups (including the American Civil Liberties Union, the Center for Democracy and Technology, and the Electronic Frontier Foundation; the Christian Coalition and the Family Research Council; the National Parent Teachers Association), lawmakers (e.g., the Congress), the Executive Branch (Department of Justice and FBI), and other interested groups.

In addition, we envision conducting two workshops within the first year in conjunction with this project. Workshops at the Academy are opportunities to convene groups of experts to address issues of pressing importance and to advise the deliberations of committees. While workshops are not intended or designed to result in consensus, findings, or recommendations, presentations and discussions at the workshops help committee members enhance their understanding of the matters before them. And, because workshops are open to the public (and in particular to staff from the executive and legislative branches), the papers presented at the workshops and the discussions conducted therein are opportunities for publicly airing information useful to the policy process before the release of a final report. (Briefing books for workshop participants containing background information, commissioned papers, and papers by speakers would also be made available to interested parties.)

One workshop will feature speakers knowledgeable about children's' use of and experiences on the Internet (at school, in the community, and at home), different non-technical approaches to the issue of protecting children from pornographic and other inappropriate material on the Internet, efforts to encourage and support children from not accessing pornographic materials on the Internet, and efforts to discourage individuals and businesses from inappropriately engaging or soliciting children on the Internet to engage in sexual activity or to view pornographic materials. This first workshop could also be used explicitly to solict the in-person views of Internet-using minors. Also, because the non-technological dimensions of the problem will change more slowly than the technologies involved, a workshop summary will be prepared that integrates the presentation of papers with the ensuing discussion. A second workshop would focus on a review of the technical options and associated operational policy considerations that can be used to help protect children from exposure to pornographic materials on the Internet, as well as the advantages and disadvantages of these options.

Depending on the availability of resources, a third workshop will be held, structured around a "design exercise" that will engage individuals from various community sectors and settings, including education; libraries; community-based agencies; churches and faith communities; business/industry, law enforcement; elected officials and other local policy makers; community leaders; parents; and teenagers. Prior to the workshop, background information would be distributed to workshop participants, describing a number of tools and strategies; this information would help to establish a common ground for workshop participants.

The "design exercise" of the workshop would involve workshop participants working in teams with representation from the various stakeholder groups (e.g., a parent, an elected official, a librarian, a teacher, a business leader, a teenager, a technologist, and a clergyperson). Each team (or teams) would be responsible for developing its own approach to protecting children from pornographic materials on the Internet, working intensively and independently for a full day. Such design exercises have the advantages that they (a) force participants from different backgrounds

440

and perspectives to interact with each other in a goal-directed manner, and (b) generate immediate feedback for ideas that result in intense, real-time scrutiny by people who understand the realities of implementation in a first-hand way.

At the end of this third workshop, the plans developed during the exercise can be compared and contrasted. As importantly, reports of the process used to generate the plan will inform the committee about potential implementation difficulties and provide greater clarity about the connection between goals and approaches.

Note that throughout the course of the project, there will be considerable effort to ensure the opportunity for public participation and comment, including public forums at the workshops, calls for public comment through the Internet and other media as appropriate, and the NRC's capabilities for accepting public input through its new interactive web pages. (Opportunities for public participation and comment will be targeted to all relevant stakeholders, including Internet-using minors.)

One unique opportunity for synergy exists with the Commission on Online Child Protection, established by the Child Online Protection Act to conduct a study regarding methods to help reduce access by minors to harmful material. The Commission's mandate to study "harmful material" is on its face broader than this study's scope and may lead it to examine many other form of inappropriate content, but the two efforts will certainly overlap with regard to access to pornographic material. While the appointment of this commission has not yet occurred, information that it develops throughout its operating life will be enormously helpful to the committee. The NRC envisions a formal liaison to this commission that will help to facilitate access to such information.

The results of the committee's deliberations will be summarized in a final report to be delivered to the sponsor 18-21 months from the date the contract is awarded. The time remaining in the 24-month project will be used for dissemination activities.

Responsiveness to the Legislative Mandate

The original legislation called for a study by the National Academy of Sciences to address four areas:

- The capabilities of present-day computer-based control technologies for controlling electronic transmission of pornographic images.
- Research needed to develop computer-based control technologies to the point of practical utility for controlling the electronic transmission of pornographic images.
- Any inherent limitations of computer-based control technologies for controlling electronic transmission of pornographic images.
- Operational policies or management techniques needed to ensure the effectiveness of these control technologies for controlling electronic transmission of pornographic images.

As noted above, a fully informed debate necessarily goes beyond technology. Thus, the study will examine the full range of tools and strategies to protect children from pornography. For example, a discussion of the capabilities of computer-based control technologies for controlling electronic transmission of pornographic images is an integral element of any discussion of filtering technologies, which will be an important element of the report. The inherent limitations of computer-based control technologies for controlling electronic transmission of pornographic images are an integral part of any discussion concerning what technology can and cannot do. Relevant operational policies or management techniques fall into the discussion of social and policy considerations in protecting children. And finally, research needed to improve computer-based control technologies will be addressed under the portion of the study that deals with a research agenda to improve tools and strategies for protecting children from inappropriate material on the Internet.

Cast in terms of discussing the risks and benefits of various tools and strategies, the findings and conclusions of the report will be aimed at informing the public policy debate at different levels (federal, state, and local) over approaches to protecting children using the Internet. Recommendations will be formulated with respect to various goals that the nation, states, school districts, libraries, and parents might decide to pursue. In other words, the report will not establish what goals any of these entities and groups should have, but rather what are more and less effective means for achieving any given goal.

Finally, the legislation calls for the study "in order to develop possible amendments to Federal criminal law and other law enforcement techniques to respond to the problem." Legislative approaches and law enforcement techniques necessary to advance the achievement of various goals will be discussed explicitly in the report.

Roles of Sponsors

A consortium of private and public funding is sought to support this study. Consistent with the NRC's mandate to seek broad public input on matters related to this study, sponsors will be approached to provide:

- briefings on areas of concern at appropriate committee meetings (and written submissions in lieu of in-person testimony);
- nominations for committee members, briefers, and reviewers, as well as for appropriate site visits and/or regional hearings;
- liaisons to relevant interest groups and stakeholders.

In addition, sponsor representatives will be invited to attend all workshops and open sessions of the committee, and will receive all briefing materials.

Product and Dissemination Plan

Using pornography and threats to children from sexual predators as the primary illustrative case, the final report for this project will include: (1) an objective description of the risks and benefits of various tools and strategies that can be used to protect children from inappropriate material on the Internet; (2) an explication of how "packages" of different tools and strategies can be used together to enable local approaches for protecting children from inappropriate material on the Internet; and (3) case studies of how different communities have approached the problem of protecting children from exposure to inappropriate material on the Internet. (However, the report will not endorse specific social goals, and thus the report will refrain from making recommendations on a specific package that should be adopted.) The report will be subject to National Research Council review procedures.

As is true of all Academy reports, an executive summary of the entire report will be prepared that highlights key findings and also specifically addresses the areas specified in the requesting legislation. In addition, a section of the report will be included that describes how the report addresses the areas mentioned in the original requesting legislation.

Workshop proceedings will be issued as interim outputs. These proceedings will include commissioned papers and briefing materials that are used to inform committee deliberations, but will not include findings, conclusions, or recommendations of the NRC. Proceedings will be made available publicly as soon as possible after the workshops involved. A summary of the first workshop will be prepared that include a synthesis of the discussions at the workshops (though again this will not include findings, conclusions, or recommendations of the NRC). (While a workshop summary is not an NRC product, the NRC will work with sponsors to develop appropriate condensations for their own use, and of course, sponsors are free to circulate these documents as they see fit.)

In order to speed the release of the report, the NRC will transmit to the sponsor and publicly release the report in pre-publication form. In content, a pre-publication report differs from a final report only with respect to copy-editing details (e.g., spelling, grammar, complete references). Both the pre-publication report and the final report are identical with respect to the analysis, findings, conclusions, and recommendations, and both are approved products of the NRC. The publication of the final report would happen several weeks later.

Dissemination activities will target two audiences: "practitioner" communities (e.g., local school systems, libraries, parents) and government policy makers (at the federal, state, and local levels) in both the legislative and executive branches. The full report is intended as a comprehensive resource to both audiences, and will be made available on the Internet via the National Academies' World Wide Web server as well as in paper form. In addition, the content of the full report will be further disseminated through participation in relevant conferences and by publication of summary articles in relevant journals, as appropriate.

In addition, the "practitioner" communities will benefit from stand-alone articles, brochures, and report extracts that pay special attention to locally implementable tools and strategies entirely apart from policy decisions that are made at higher levels. Such materials would be oriented towards what these people can do -- as individuals and local communities -- to help protect children on the Internet.

Public Information About the Project

The Academy will post on its Web site (http://www.nationalacademies.org) a brief description of the project, as well as committee appointments, if any, with short biographies of the members, meeting notices, and other pertinent information, to afford the public greater knowledge of Academy activities, and an opportunity to make comments. The Web site will also include the project's on-going record of compliance with the requirements of Section 15 of the Federal Advisory Committee Act, 5 U.S.C. App. § 15. Sponsors will be provided compliance certification(s) in accordance with Academy procedures.

NOTES:

(1) According to the Department of Education, the fraction of U.S. schools with access to the Internet grew from 35% in 1994 to 89% in 1998, while the comparable fraction of U.S. classrooms rose from 3% in 1994 to 51% in 1998. See *Internet Access in Public Schools and Classrooms: 1994-1998*, U.S. Department of Education, National Center for Educational Statistics, 1999.

(2) According to the National Telecommunications and Information Administration of the Department of Commerce, 36.6% of the U.S. population have personal computers (PCs), 26.3% have modems, and 18.6% have on-line access. See *Falling Through the Net II: New Data on the Digital Divide*, available from http://www.ntia.doc.gov/ntiahome/net2/falling.html. Released July 1998.

(3) A recent study from the Annenberg Public Policy Center Found that parents in the U.S. are deeply fearful about the Internet's influence on their children while at the same time believing that

the Internet has important and positive educational potential. See Joseph Turow, *The Internet and the Family:The View from Parents, The View from the Press*, Annenberg Public Policy Center, University of Pennsylvania, May 1999

(4) Lawrence Lessig and Paul Resnick, "The Architectures of Mandated Access Controls," Paper presented at the Telecommunications Policy Research Conference, October 4, 1998. See http://www.si.umich.edu/~prie/tprc/agenda98.html.

(5) PICS is part of a larger effort being managed by the World Wide Web Consortium on metadata, that is, data associated with Web content that represents information about that content in a way that is easy for machines to deal with. Metadata is intended to facilitate searching, helping authors to describe their documents in ways that search engines, browsers and Web crawlers can understand. The approach embodied in PICS has both supporters (e.g., Paul Resnick, "Filtering Information on the Internet", *Scientific American*, March 1997), and detractors (e.g., Lawrence Lessig, "Tyranny in the Infrastructure", *Wired*, July 1997).

(6) In this nomenclature, "tools" refer to technological means for protecting children from pornographic and other inappropriate materials on the Internet, while "strategies" refer to actions to promote or enhance such protection that can be taken by key stakeholders in the lives of children, such as parents, teaches, librarians, and federal, state, and local policy makers.

(7) In the non-networked world, such techniques include movie ratings, special (restricted) sections of video and book stores, opaque covers over pornographic magazine covers, reporting to law enforcement officials of suspected child pornographers by photo processing lab personnel, special hours of or channels for broadcast of certain cable TV shows, and so on.

Tentative Project Schedule

Month 1	Meeting 1 Briefings for the committee are open to interested parties.
Month 3	Meeting 2: Workshop #1 for 1_ days; meeting for 1_ days Workshop topics (public workshop) • Patterns of children's use of the Internet • Non-technical options for protecting children on the Internet, including acceptable use policies; parental guidance; safety education (for example) Non-workshop briefings for the committee held during the meeting are open to interested parties. Workshop briefing books (background materials, commissioned papers, workshop papers if available) will be made available to sponsors immediately.
Month 6	Meeting 3: Workshop #2 for 1_ days; meeting for 1_ days Workshop topics (public workshop) • Technical options for protecting children on the Internet, including mechanisms for filtering and age verification (for example) • Operational policy considerations needed to support various technical options Non-workshop briefings for the committee held during the meeting are open to interested parties. Workshop briefing books (background materials, commissioned papers, workshop papers if available) will be made available to sponsors immediately.
Month 7	Workshop #1 summary (including workshop discussions) delivered to sponsor
Month 10	Workshop #2 summary (including workshop discussions) delivered to sponsor
Months 7-10	Regional hearings and site visits for more gathering of information
Month 11	Meeting 4: meeting for 3 days Briefings for the committee are open to interested parties.
Month 13	Meeting 5: meeting for 3 days

	Briefings for the committee are open to interested parties.
Month 15	Meeting 6: meeting for 3 days (probably closed meeting)
Month 18	Report release (in pre-publication form); paperless briefings for sponsor in advance of public release.
Months 19-24	Dissemination efforts, including • Writing of pieces for practitioners (teachers, librarians, parents, IT vendors) • Issuing final report in book form

Public Law 105-314
Protection of Children from Sexual Predators Act of 1998
Title IX, Section 901

SEC. 901. STUDY ON LIMITING THE AVAILABILITY OF PORNOGRAPHY ON THE INTERNET.

(a) IN GENERAL- Not later than 90 days after the date of enactment of this Act, the Attorney General shall request that the National Academy of Sciences, acting through its National Research Council, enter into a contract to conduct a study of computer-based technologies and other approaches to the problem of the availability of pornographic material to children on the Internet, in order to develop possible amendments to Federal criminal law and other law enforcement techniques to respond to the problem.

(b) CONTENTS OF STUDY- The study under this section shall address each of the following:

(1) The capabilities of present-day computer-based control technologies for controlling electronic transmission of pornographic images.

(2) Research needed to develop computer-based control technologies to the point of practical utility for controlling the electronic transmission of pornographic images.

(3) Any inherent limitations of computer-based control technologies for controlling electronic transmission of pornographic images.

(4) Operational policies or management techniques needed to ensure the effectiveness of these control technologies for controlling electronic transmission of pornographic images.

(c) FINAL REPORT- Not later than 2 years after the date of enactment of this Act, the Attorney General shall submit to the Committees on the Judiciary of the House of Representatives and the Senate a final report of the study under this section, which report shall--

(1) set forth the findings, conclusions, and recommendations of the Council; and

(2) be submitted by the Committees on the Judiciary of the House of Representatives and the Senate to relevant Government agencies and committees of Congress.

Christopher D. Hunter is a Ph.D. candidate at the Annenberg School for Communication of the University of Pennsylvania, where he received his MA degree in 1999. Hunter received his BA from Boston College in 1997, graduating with summa cum laude and Phi Beta Kappa honors. Hunter's MA thesis, "Filtering the Future? : Software Filters, Porn, PICS, and the Internet Content Conundrum," focused on the public policy implications of Internet filtering and rating technologies. An empirical analysis of filter performance included in the thesis was awarded the Most Outstanding Student Paper award at the 2000 Computers, Freedom and Privacy Conference, and was recently published in the Summer 2000 volume of the respected journal, the "Social Science Computer Review." Hunter's current research focuses on ways to improve the empirical analysis of filter performance, and the dynamics of filter adoption and use by families, schools, and libraries.

Contact Information
phone: (215) 732-4612
email: chunter@asc.upenn.edu
web: http://www.asc.upenn.edu/usr/chunter/

COPA Commission Testimony

On July 20th in Richmond, Virginia I had the opportunity to testify before the Congressionally appointed COPA Commission about the effectiveness and first amendment implications of Internet content filtering and rating software. Below is my opening statement and extended answers to the commission's questions.

- COPA Commission Opening Statement [html, pdf]

-Responses to the COPA Commission Questions Regarding Internet Filtering, Labeling, and Rating Technologies [html, pdf]

Christopher D. Hunter
Ph.D. Candidate
Annenberg School for Communication
University of Pennsylvania
chunter@asc.upenn.edu
http://www.asc.upenn.edu/usr/chunter/

COPA Commission Opening Statements

July 20, 2000

Christopher D. Hunter
Ph.D. Candidate
Annenberg School for Communication
University of Pennsylvania
215-732-4612
chunter@asc.upenn.edu

I would like to thank the members of the COPA Commission for inviting me here today. It is an honor to be able to present my research into the effectiveness of software filters, Internet content ratings systems, and the adoption, or lack thereof, of these technologies.

I would like to make two points in my brief testimony this afternoon; 1) parents fear the Internet but they trust their children, and 2) we need more open and rigorous empirical analyses of software filter performance.

Parents Fear the Internet But Trust Their Children

The prime reason we are here today is because parents have expressed a great deal of anxiety about the "dark corners" and "red light districts" of the Internet. Numerous national surveys have identified a high level of parental fear. Through survey research led by Dr. Joseph Turow of the Annenberg Public Policy Center of the University of Pennsylvania, we have tried to move beyond the issue of fear alone, to better understand the complex dynamics of family Internet use.

In two nationally representative surveys, one conducted in December 1998, the other completed in February of this year, we again found that parents are very concerned about inappropriate Internet content. Our 1998 study found that 76% of parents agreed with the statement "I am concerned that my child might view sexually explicit images on the Internet," and 60% felt that the Internet was an unsafe place for their children to spend time. Our 2000 follow up survey found that 72% of parents feared their children might be exposed to sexually explicit images on the Internet, and 50% felt the net was an unsafe place for their children. Despite these high levels of concern, we found that a minority of parents have actually adopted Internet filtering software. Only 32% of parents in the 1998 survey, and only 18% of parents in the 2000 survey reported using filtering software to shield their children from harmful Internet material.

What explains the large gap between parents fears and the adoption of filtering software so often promoted as the best solution for protecting children on the Internet? One might think that this is due to a lack of awareness among parents, however our 2000 survey found that 79% of parents had heard of filtering software. Interestingly, even among parents aware of filters, only 25% reported using such software.

I think a better explanation is the somewhat surprising finding that a majority of parents completely trust their childrens online behavior. Our 1998 survey found that 58% of parents of 8-12 year olds, and 61% of parents of 13-17 year olds, said they had complete trust in their child's online behavior. Among all child age groups in the 2000 survey, 54% of parents reported complete trust in their child's Internet use, and 35% reported being somewhat trusting. These results led my professor Joe Turow to conclude that "while parents trust their children, they do not trust the web."

One reason that parents likely trust their children is that parents have adopted a number of simple, sensible, non-technical rules about when, where, and how their children can use the Internet. Our 1998 survey found large percentages of parents employing the following simple methods for monitoring online use:

- The sites children view online
- The time of day or night a child is allowed to go online
- The kind of activities the child performs online
- The amount of time spent online

- Going online only with an adult, be it from home or outside of the home

These results should remind us that parents have already discovered methods which work well in protecting children from inappropriate Internet content. All to often in public policy debates about children and Internet content appropriateness we come to the knee-jerk conclusion that technology is the answer. However, instead of solely promoting technological solutions like filters and content rating systems, perhaps we should focus more attention on the simple yet effective methods that parents are already widely using.

The Need for More Filter Effectiveness Studies

Filters have been promoted by many as an effective and First Amendment friendly tool for keeping kids away from objectionable Internet material while at the same time not blocking access to useful and benign information. Unfortunately, a number of studies conducted by a wide range of groups including Consumer Reports, the Center for Media Education, the Electronic Privacy Information Center, the Censorware Project, and Peacefire have found that filters are not as effective as advertised. These studies have tended to find two types of filter errors. First, filters have often been found to let through pornography, violence, and hate speech related web sites, the very types of content these products are meant to block. Secondly, and more troublesome from a First Amendment standpoint, filters have been found to block access to perfectly benign material including web sites related to the Declaration of Independence, the U.S. Constitution, and the Bible. Many left leaning political groups and gay and lesbian related sites are also systematically blocked by a number of filters.

In my own research I have attempted to develop a more systematic methodological framework for analyzing filter performance. I think three aspects are absolutely critical in this regard:

> 1. We need to be able to make reliable generalizations about the types of content that filters should and should not block access to. To achieve this, I suggest the use of content analysis of web sites using a clear and reliable rating system geared towards Internet content. To date, I have used RSACi as my rating system, but any number of other coding systems would also be appropriate.
>
> 2. We need samples of web content which reflect the surfing patterns of users in different contexts; home use, school use, library use, etc. Testing filters against these samples allows us to infer their effectiveness within these very different contexts. My own research has attempted to replicate the surfing patterns of home Internet users serendipitously surfing the net, using search engines, and using directory sites like Yahoo! .
>
> 3. The results of any analysis should be completely open to scrutiny. Every web site sample selected, every rating decision, and every site blocked by every filter tested should be available in some sort of public master list. The more open the methods, the less likely results will be jury-rigged. Open methods also allow other researchers to conduct similar studies to confirm the results of any one filter performance test.

Using the methods listed above on a sample of 200 web sites, I found that the combined performance of four popular client-side filtering programs was quite poor as they failed to block objectionable content 25% of the time, while incorrectly blocking benign content 21% of the time. These results have led me to the conclusion that filters are a flawed solution, particularly in the context of libraries, for protecting children from harmful Internet content, while not limiting access to legitimate information.

There are limitations to my study, namely that I tested only client-side filters, limited generalizability due to the lack of a truly random sample, and the failure of RSACi to capture some types of content that parents might find objectionable. I have attempted to address these limitations in my "Cyberporn, Filters, and Public Policy: A Content Analysis Research Proposal," which is available for download on the COPA Commission web site. Using my proposed methodology, or one similar to it, I am confident that filter effectiveness can be empirically tested in a fair and open fashion. It is my hope that a great many more studies of filter effectiveness will be conducted in the near future. I think a relatively uncontentious and sensible recommendation that this commission can make is that the National Academy of Science and the National Science Foundation should fund non-partisan research into filter effectiveness.

Conclusion

The survey work and filter effectiveness studies I have just cited, lead me to conclude that software filters and Internet content rating systems, at least as they are currently configured, are not the optimal solution for protecting children from harmful Internet material. Filters and Internet rating systems are a seductively simple solution which promise to solve a long standing problem by simply installing a piece of software. It is my contention however that complex social problems can not be reduced to lines of code. Rather, social problems call for social solutions, and in my mind the most effective and contextually sensitive filtering and rating system ever devised is a concerned parent taking the time to surf the Internet with his/her child.

Responses to the COPA Commission Questions Regarding Internet Filtering, Labeling, and Rating Technologies

July 18, 2000

Christopher D. Hunter
Ph.D. Candidate
Annenberg School for Communication
University of Pennsylvania
215-732-4612

chunter@asc.upenn.edu
http://www.asc.upenn.edu/usr/chunter/

1. What information exists regarding parents' awareness and attitudes about Internet filtering?

There is a good deal of credible survey evidence which shows that while parents do indeed fear the "dark corners" of the Internet, relatively few have installed filtering software to protect their children from this perceived danger. The best evidence of this rather counterintuitive finding comes from a number of nationally representative surveys conducted by the Annenberg Public Policy Center of the University of Pennsylvania. In a survey conducted in December 1998, Dr. Joseph Turow found that while 76% of parents agreed with the statement "I am concerned that my child might view sexually explicit images on the Internet," and 60% felt that the Internet was an unsafe place for their children to spend time, only 32% of parents with Internet access used filtering software (Turow, 1999). In a follow up survey conducted in January and February of this year, 72% of parents feared their children might be exposed to sexually explicit images on the Internet, and 50% felt the net was an unsafe place for their children, but only 18% reported using filtering software (Turow and Nir, 2000). These results are summarized in Table 1.

Table 1: Annenberg Survey Results

	1998 Survey Agree	2000 Survey Agree
I am concerned that my child might view sexually explicit images on the Internet.	76%	72%
The Internet is a safe place for my children to spend time.	40%	50%
Use filtering software	32%	18%

Finally, in yet another survey conducted by the Annenberg Public Policy Center in April and May of this year, Dr. Emory Woodard found that 32% of families with Internet access used Internet filtering software (Woodard, 2000).

If parents are so concerned with the dangers of the Internet, why are relatively few using filtering software often advertised by filter makers, parents groups, and legislators as the best solution to the problem of objectionable Internet content? One possible explanation is that parents are not aware of the existence of filtering software. However, the results from the Turow and Nir 2000 study show that a large majority, 79% of parents with Internet access, are aware of Internet filters. Interestingly, among parents aware of filters, a minority, only 25% actually use such programs.

Another possible explanation for the gap between parents fears and actual filter use, is a phenomena known as the third-person effect, which finds that "individuals exposed to a mass media message will expect the communication to have a greater effect on others than on themselves (Davison, 1983)." In simple English, parents are likely to fear the dangerous effects of the Internet in general, but are confident that it wont harm their children. Indirect evidence supporting this hypothesis can be found in Turow's 1998 and 2000 surveys. In the 1998 survey, 58% of parents of 8-12 year olds, and 61% of parents of 13-17 year olds, said they had complete trust in their child's online behavior. Among all child age groups in the 2000 survey, 54% of parents reported complete trust in their child's Internet use, and 35% reported being somewhat trusting. While these results point to some tentative support for a third-person-like effect, more systematic survey work is needed to test this hypothesis. A reasonable conclusion that can be reached from this data is that "while parents trust their children, they do not trust the web (Turow, 1999: 19)."

A final possible explanation for a lack of filter use, is that parents feel they have the situation well in hand due to their reliance on traditional, non-technical media usage rules. In Turow's 1998 survey, large percentages of parents indicated that they set rules regarding online use such as time restrictions and Internet use only in the presence of a parent. The Woodard 2000 survey found similar Internet use rules.

The results presented above suggest that parents may be more confident and in control of their childrens Internet use than a simple "are you afraid of the Internet" question might imply. Also, by exclusively focusing on technical means to protect children, this commission may well be overlooking simple yet effective non-technical rules that parents are already widely using.

2. What is the relevance of traditional labeling or rating of movies, tv shows and video games to the Internet?

There is no question that content rating/labeling systems have become a reality for many forms of mass entertainment including movies, music recordings, television, and video games. Given the successful implementation of content labels in the "real world", many scholars and public policy advocates have argued for a similar rating system for Internet content. While such proposals seem simple and reasonable, traditional rating systems nevertheless raise a number of difficult practical and constitutional issues that will likely also apply to any proposed Internet content rating system.

On the practical side of the ratings debate, there are questions about just how useful rating systems are for concerned parents. Many proponents of content rating claim that such systems help inform parents about their childrens media use. But just how informative are current rating systems? With regards to the Motion Picture Association of America's (MPAA) rating system (around since 1968), there is little question that parents find it informative. In a 1999 study conducted by the Kaiser Family Foundation, 82% of parents reported using the system to guide their family viewing choices. The situation is less clear for music labels and ratings for tv shows. The same Kaiser study found that only 42% of parents used parental advisory labels on CD's and only 52% of parents utilized tv ratings in guiding family viewing (Kaiser, 1999). Further evidence of the limited informational value of tv ratings is found in the Annenberg Public Policy Center's *Media in the Home 2000* study, which found that 50% of parents were aware of tv ratings, and that only 39% of parents reported using the ratings to guide their childrens viewing (Woodard, 2000). The Annenberg study also found that only 51% of parents with V-chip enabled televisions were actually utilizing the technology.

These statistics raise questions about the informational utility of content rating systems. Questions however do remain if this is due to a lack of education/awareness among parents about the systems, or whether parents simply ignore content labels as uninformative and unlikely to actually aide them in controlling family viewing behavior. Further survey work similar to the Kaiser and Annenberg studies will be vital in answering these questions.

From a Constitutional and free speech perspective, content rating systems raise serious questions about governmental imposition of values on the private sector and the creation of a slippery slope which will inevitably lead to the outright censorship of unpopular/controversial, but nevertheless protected First Amendment speech. While proponents of content labeling claim that such systems are "voluntary," in nearly every instance media industries have adopted rating systems under threat of direct government regulation. An excellent example of this is the current tv rating system which came about because Congress essentially told the television industry that if they did not create an acceptable system (acceptable that is to the FCC, Sen. John McCain, and Sen. Joseph Lieberman, in other words, the government), that it would impose its own system. Such strong arm tactics raise the question of just how voluntary a system is where the government tells you "do this or else?" As First Amendment lawyer Robert Corn-Revere has noted, Congress "tried to cast this as a voluntary effort, but what they are really saying is, 'Do it to yourself, or we'll pull the trigger (in Taylor, 1999).'"

Rodney Smolla makes a similar point, commenting that "If there is a case to be made against what the FCC did with regards to children's television, it must be not the goal but the method of using governmental power and leverage to exact concessions from the private sector (1997)."

Once industry concessions in the form of ratings are made, proponents claim that content labels will merely be used to "provide information for parents (cited in Roberts, 1997)." However, such systems have been combined with market forces and state regulations to outright censor media content. In the U.S. record industry, about 10% of all music is sold by Walmart, which will not carry records that have advisory labels. This has forced many popular musicians to rewrite their songs in order to be "approved" by Walmart. Similarly, several states including Georgia, Washington, and Tennessee have attempted to pass laws banning the sale of labeled records to minors. As Lasica notes, Parental Advisory Labels which "started out as a tool for parental empowerment turned into an effective means of censorship (1997)." A similar situation has occurred in the movie industry where any film given an NC-17 rating will not be carried by theaters. This has led numerous directors to "soften" their work to receive an acceptable R-rating (Taylor, 1998). Additionally, many states periodically entertain legislation that would make it illegal for underage children to be admitted to R-rated films. Such legislation is patently unconstitutional, as it essentially outsources the careful and precise rules that government must follow to limit speech, to the vague rules used by the MPAA. As a federal court in the case of *Swope v. Lubbers* (1983), concluded "it is well-established that the Motion Picture ratings may not be used as a standard for a determination of constitutional status."

The situation outlined above suggests that supposedly "informational" and "voluntary" rating systems are likely to lead to mandatory labeling and state sanctioned censorship based on such labels. Evidence of this trend extending to Internet content rating systems can already be seen in the European Union's plans to control "harmful" Internet material. The EU is directly funding efforts to develop a new Internet content rating system as well as interoperable filters. A rough sketch of the EU's plans is provided by the Bertelsmann Foundation's "Self-regulation of Internet Content" proposal, released in September 1999. Given that the EU is directly funding this effort, it is a quite a stretch to call it "voluntary self-regulation." Similar proposals which mandate rating and filtering Internet content have been proposed in Australia, China, and Singapore.

3. What information exists regarding parents' awareness and attitudes about Internet filtering, rating/labeling?

For information about parents awareness and attitudes towards filtering software, see response my to question one.

There is relatively little evidence regarding parents awareness, attitudes, and use of Internet content rating/labeling systems. What evidence does exist, suggest that parents do support the idea of Internet content labeling, but are largely unaware of current rating systems such as RSACi and SafeSurf.

In a June 1999, multinational survey sponsored by the Bertelsmann Foundation, 69% of all U.S. respondents, and 75% of U.S. respondents with children under 18 reported that they would find some type of Internet rating system useful. In the 1999 Kaiser Family Foundation survey mentioned earlier, only 29% of all parents, and only 39% of parents with Internet access said they had used an Internet rating system to help guide their children's surfing behavior. Low awareness and use of Internet content rating systems is likely due to the fact that such systems are relatively new, and have not received nearly as much attention as popular content blocking software like Cyber Patrol and SurfWatch.

Both Microsoft and Netscape/AOL have integrated PICS-based filtering modules into their browser software, however neither company has released statistics on what percentage of their users have activated these tools, or what settings the average user employs. Such information would be highly valuable to the policy community in assessing the utility of label-based filtering and for understanding the extent to which labeled (or unlabeled) Internet content would be blocked by these systems.

4. What legislation would be most appropriate to promote awareness and effective use of filtering, rating/labeling?

There is absolutely no need for legislation which implicitly endorses filters and rating systems through the very fact that they are being promoted by the federal government. The Internet industry has already responded to parents demands for information about filters and rating systems through information kits distributed by Internet Service Providers, and joint efforts such as the GetNetWise web site (http://www.getnetwise.org/) which lists hundreds of tools and techniques for protecting children on the net.

5. Should government conduct, sponsor or fund research into improving filtering, labeling and rating systems?

The government does have a legitimate role in funding rigorous, non-partisan research into the effectiveness and use of Internet filtering and rating technologies. The current public policy debate about filtering technology would be greatly improved if more systematic studies of filter performance were available. To date most studies of filter performance have been produced by the filter makers themselves or by groups often perceived as having some bias, both pro and anti-filter. To the extent that dispassionate and objective research on an issue as politically charged as protecting children from pornography, hate speech, etc. is possible, the federal government through research agencies such as the General Accounting Office (GAO), the National Academy of Sciences (NAS) and the National Science Foundation (NSF) should sponsor studies of filter effectiveness. The current NAS project on "Tools and Strategies for Protecting Kids from Pornography and Their Applicability to Other Inappropriate Internet Content" is a promising first step in this direction.

The NAS and NSF should also consider funding research which investigates how parents use or do not use filtering and rating technologies. All to often the public policy community simply assumes that if a technology exists to "solve" a particular problem, people will naturally use it. However, user studies often find that people are not inclined to use technological solutions (perhaps due to complexity or time restraints) and instead rely on other methods, rules, etc. If research finds that parents are not inclined to use filter and rating/labeling software, but instead find traditional rule setting methods adequate, there would seem little sense in promoting the technology as a "solution" to parents fears.

Thus the role of empirical research in the current filtering debate will be to replace unscientific assumptions about filter performance and use, with rigorous social science evidence.

6. Must a filtering, labeling or rating system be international in order to be effective?

The Internet is an inherently global network. Information on a web server in Kiev is just as accessible as information on a web sever in Kalamazoo. This reality has led many scholars to call the net a borderless medium (Johnson & Post , 1996). While U.S. users and content still dominate the Internet -- 85% of web pages originate in the U.S. vs. only 15% from abroad (Cyveillance, 2000) -- this is rapidly changing. According to estimates by TechServer, by 2003 non-English language material will account for more than half of the content published on the web, much of this originating from international web servers (in NUA, 1999). In addition, by 2003 U.S. users will account for less than one-third of the worldwide population of Internet users (IDC, 1999). As more and more international users come online, the growth in foreign based content will continue to explode.

Given the international reality of the net, and the fact that in the near future, U.S. users will likely be surfing to many foreign web sites, and vice versa, some form of international cooperation will be needed to develop a rating system with some baseline agreements about what content should be labeled as pornographic, violent, hateful, etc. Currently, the Internet Content Rating Association (ICRA) and Internet Content Rating for Europe (INCORE) group are attempting to develop just such a system, but they face a difficult if not impossible task.

The idea that the nations of the world, with their tremendous diversity and multiplicity of ethnic, cultural, and religious beliefs could agree on a single standard or set of definitions for what constitutes foul language, nudity, pornography, or violence seems at best wishful thinking, and at worse just plain ludicrous. We need only look to our own tortured experience in attempting to define pornography vs. erotica vs. great literature, a pursuit which bedeviled the Supreme Court for the better part of the 20th century (Kendrick, 1987), to see the difficulty in achieving a truly international rating system. The difficulty in reaching international consensus on what information should be rated and blocked is well illustrated by the 1999 Bertelsmann international risk assessment survey. It found that only 13% of Germans thought nudity should be banned from the net in contrast to 43% of Americans. The situation is reversed for violent content which only 39% of Americans felt should be banned vs. 61% of Germans. Finally, 58% of Germans felt that radical right and left wing political content (whatever that means?) should be blocked, vs. only 26% of Americans (Bertelsmann, 1999).

These deeply rooted cultural differences about what constitutes harmful content may well undermine the reliable application of any Internet rating system. For example, imagine that a web page developer in Germany has posted a page with pictures of nude women. Since German's seem to be less offended by nudity, the site developer would be inclined to rate his/her site as inoffensive. This would stand in contrast to the expectation of U.S. users who are generally offended by nudity, and would have expected the German page to be rated as offensive. Multiply this scenario out over disagreements about how to rate for violence, hate speech, offensive language, etc., and we can see why a reliable international rating system is highly unlikely.

7. What are the implications of filtering and labeling technologies for privacy, first amendment rights, and law enforcement?

First Amendment Implications of Filters

The first amendment problems associated with installing filters in public libraries and schools have been well documented by the American Civil Liberties Union (1997; 1998), the American Library Association (1997), and Jonathan Wallace of the Censorware Project (1997). The crux of the problem is that when libraries purchase access to the Internet they are essentially acquiring the entire contents of the net, or by analogy a near infinite book collection, or the worlds largest encyclopedia. Once purchased, libraries can not simply remove books because they contain disfavored content. As the Supreme Court ruled in the case of *Island Trees Board of Education v. Pico* (1982), "In brief, we hold that local school boards may not remove books from school library shelves simply because they dislike the ideas contained in those books and seek by their removal to 'prescribe what shall be orthodox in politics, nationalism, religion, or other matters of opinion.'" When a filter blocks a web site, it is analogous to removing a book from a library, and therefore presumtively unconstitutional.

Even if a library had a legitimate purpose for restricting access to otherwise protected speech, such limitations would need to meet the very high "strict scrutiny" standard, which requires the government to prove that its restrictions on protected speech are narrowly tailored to meet a compelling government interest. Filters can not live up to this standard as their rules for blocking content are inherently vague and overbroad. Making things worse, most filter makers refuse to reveal the lists of sites they block and the specific criteria which leads to a decision to deny access to a web site. Because of these vague rules, libraries can not escape their constitutional requirements by outsourcing decisions about content appropriateness to secretive filter makers.

The logic of these arguments was largely adopted by the court in the case of *Mainstream Loudoun, et. al. v. Board of Trustees of the Loudoun County Library* (1998) which found that a local library's ordinance requiring filters on all public terminals was an unconstitutional abridgment of patrons first amendment rights. In a strongly worded rebuke of the Loudoun County filtering policy, Judge Brinkema noted the absurdity of outsourcing decisions about content appropriateness to a secretive filter maker:

> The degree to which the policy is completely lacking in standards is demonstrated by the defendant's willingness to entrust all preliminary blocking decisions -- and, by default, the overwhelming majority of final decisions -- to a private vendor, Log-On Data Corp. Although the defendant argues that X-Stop is the best available filter, a defendant cannot avoid its constitutional obligation by contracting out its decision making to a private entity. Such abdication of its obligation is made even worse by the undisputed facts here. Specifically, defendant concedes that it does not know the criteria by which Log-On Data makes its blocking decisions. It is also undisputed that Log-On Data does not base its blocking decisions on any legal definition of obscenity or even on the parameters of defendant's policy.

The *Loudoun* decision essentially says that filtered access on *all* public library terminals will likely be found unconstitutional. Left unanswered by the decision is the equally difficult question of whether filtered access on child only computers would be permissible. The Supreme Court has found that minors do have a constitutional right to access protected speech. As such, would filters violate a teenager's right to access safe sex information, or web sites devoted to helping gay and lesbian teens confused about their sexuality, two types of sites that filters have been found to frequently block? These questions remain unanswered and will likely only be resolved in a court challenge.

Many of the arguments brought up in the *Loudoun* decision would also likely apply to a court challenge of public school mandated filtering. However, because the courts have given schools wide discretion in curricular and disciplinary decision making, it is unclear under what circumstances filters would be permitted. The *Pico* case would seem to imply that school administrators can filter access to the Internet if it is part of a predefined classroom curriculum. In essence, filters would mirror a school board's power to decide what text books are appropriate. However, if schools grant students unsupervised time to simply "surf the net" for research purposes, therefore not part of a predefined lesson plan, than filtering would not be permissible. As Kubota (1997) notes, "The freedom of choice enjoyed by students while browsing the Internet is analogous to students searching the library and voluntarily choosing bocks of interest. Schools can not claim to have any real curricular control over such an open-ended, free wheeling, and unsupervised activity (713)."

First Amendment Implications of Rating/Labeling Systems

The first amendment problems associated with Internet content rating/labeling systems were noted above in my response to question two. Basically the fear is that supposedly "voluntary" and "informational" systems will inevitably lead to government mandated labeling and censorship based on such labels. Our experience with MPAA ratings and Parental Advisory labels show that such concerns are not without merit. Indeed, in 1997 when President Clinton convened an "Internet summit" on how to protect children from harmful Internet content, the SafeSurf group proposed the "Online Cooperative Publishing Act" which would have required certain web publishers to self-rate, and would have allowed for fines against sites which refused to rate or mislabeled their content (SafeSurf, 1997). Fortunately, laws requiring such labels are likely to be found an unconstitutional form of forced speech (see *Riley v. National Federation of the Bline* and *McIntyre v. Ohio Elections Commission*).

Another potential problem with rating systems is overbreadth. For label-based filtering products to be truly effective they need to block all unrated web sites. Given that there is a highly uneven incentive structure for web developers to self-rate -- commercial developers are far more likely than non-commercial or individual web developers to bother with self-rating (Weinberg, 1997) -- it is entirely likely that label-based filters will block a great deal of idiosyncratic speech. The end result of blocking unrated web sites would be a homogenized Internet that reflects the interests of gigantic advertiser driven media/entertainment portals and e-commerce sites, a situation I like to call the "malling of the net." Joseph Lasica (1997) makes a similar point about blocking unrated web sites, noting:

> Internet ratings dovetail nicely with big business's desire to make the Internet safe for God, apple pie and commercialism. The "dark side" of the net -- hackers, foreigners, political extremists, geeks, phreaks, porn purveyors, hate groups, people who SHOUT IN ALL CAPS AND USE EXCLAMATION MARKS!!! -- will largely be banished to an unrated no-man's land where browsers and search engines fear to tread.

While this process, if carried out solely by the private sector, would not raise constitutional issues per say, it would still seem to fall outside of our first amendment tradition which promotes the notion of an open, diverse, even rambunctious "marketplace of ideas." Nadine Strossen of the ACLU makes a similar point, noting that "calling upon Internet content providers and speakers to 'self-rate' their expression is no less contrary to the basic principles of free expression than a proposal that publishers of books or magazines 'self-rate' their publications, including all stories and articles, or a proposal that participants in street corner conversations rate their oral statements (1999)." Donald Haines, also of the ACLU, amplifies Strossen's last point, "Imagine being forced to wear a sandwich board that says 'violent and sexual content' if you want to stand on the street and hand out a pamphlet on domestic abuse (1997)."

8. How do current filter systems operate, and to what extent do they rely on rating and labeling?

Currently available filtering products use a wide range of techniques (blacklists, whitelists, key word filtering, label-based filtering, customer reports, etc.) to find, classify, and block objectionable/harmful Internet content. The most commonly used of these methods is the development of extensive black lists which contain hundreds of thousands of blocked web sites, web pages, usenet newsgroups, and mailing lists. These lists are compiled using two primary methods. The first method is human review, in which companies hire "professional surfers" to surf the net looking for objectionable content. When material which meets a filter maker's blocking criteria is found, the web site, newsgroup, etc. is added to the programs master black list. Many filter makers claim that all of their blocking decisions are based on careful human review, but this claim is somewhat suspect. Put simply the web is a vast space. There are currently more than 17 million web sites (Netcraft, 2000), and 2.1 billion unique, publicly available web pages (Cyveillance, 2000). In addition, every day 7 million web pages are created, and some 50 million existing pages change their content (Censorware Project, 2000). Combining the shear size of the web, with its ever changing nature, it is clearly impossible for any filter company, even with a staff of hundreds or even thousands, to review a majority of the web's content for pornographic material. This reality sheds doubt on some filter makers claims that their software rates 90-95 percent of the web. Further, even if they were able to review such a large percent of web content, they would have to continually re-review sites that have updated their content (for example candyland.com was originally a pornography web site until Hasbro bought the domain and converted it to a Candyland board game product site). Because it is simply impossible for human reviewers to keep up with the ever growing web, filter companies must resort to the use of context insensitive web spiders, which block content due to the presence of key words like sex, breast, etc. Context insensitive blocking via automated spiders is one of the primary reasons for over-filtering (discussed further below).

Another measure which many filter programs employ is key word filtering. If a site does not appear on the blocked sites list, many filter programs will still "read" the page before it is displayed by a web browser. If the filter encounters key words which have been deemed improper it will either block out those words, or completely deny access to the page. Unfortunately, word filters are rarely advanced enough to understand context, and thus block out words such as "Essex" and "Anne Sexton" because they contain the dirty little word "sex." In one hilarious example of this problem, CYBERsitter's blocking of the word "homosexual" would render "President Clinton opposes homosexual marriage" to say "President Clinton opposes marriage (Weinberg, 1997)." Similarly, at one point AOL got into trouble for blocking the word "breast", thus also forbidding "chicken breast", "turkey breast," and more importantly "breast cancer ." More recently, AOL has been chided for pointing customers of its ICQ chat service, to download a very conservative word filter offered by the ClickChoice Company. Its DirtyWords filter blocks out your usual sexual oriented terms, but also goes much further to block "popculture, lesbian, accounting.com, safesex, and now.org ." Finally, Net Nanny makes the FCC and

George Carlin's "seven dirty words" look quaint with its list of 118 off-limits words (see Table 2)! In addition to the usual sexually oriented terms Net Nanny also finds fault with "anarchy" and "spunk"?

Table 2: NetNanny Blocked Words List (May 1999)

Adult Check
adult entertainment
adult gif
Adult ID
adult images
adult links
adult movies
adult pics
AdultCheck
AdultSights
amateur sex
amateur videos
amateur women
anal
anarchy
ass
asshole
beastiality
bestiality
blowjob
blowjobs
bomb
bondage
boob
buttfucking
cannibalism
clit
cock
cocks
coitus
copulate
copulation
cum
cumshot
cumshots
cunnilingus
cunt
cunts
dicks
dildo
dildos
doobie
drugs
ejaculate
ejaculation
erection
erotic
erotica
exhibitionism
exhibitionist
exhibitionists
fellatio
fetish
fistfuck
fisting
flesh
fuck
fucked
fuckers
fucking
gangbang
groupsex
hard-on
hardcore
hardon
horniest
horny
incest
intercourse
jism
kinky
live couples
lust nudity
lusting
marijuana
masturbate
masturbation
nude
nudes
nudity
nympho
nymphomania
nymphomaniac
oral
orgasm
orgy
penis
perversion
perverted
porn
porno
pornography
prick
pussies
pussy screw
S&M
screwing
sex
sex toys
sexual
sexually
slut
sluts
smut
spunk
suck
teen movies
teen pics
teen videos
threesome
tit
tits
twat
voyeurism
whore
XXX
zoophile
zoophilia

To what extent do filters rely on rating and labeling?

A number of popular filtering programs including Cyber Patrol, CYBERsitter, and SurfWatch include PICS compliant modules. More importantly, both Netscape and Microsoft browsers contain PICS-based filter modules, which means that roughly 90% of web surfers have access to label-based filtering. Despite the fact that a number of filter products have integrated label-based filtering, these modules are of relatively little use because a very small minority of web sites have self-rated using RSACi, SafeSurf, or some other rating system. Indeed, less than 200,000 web sites (or about 1% of total web sites) have self-rated using the industry leading RSACi system.

9. What evidence exists regarding the effectiveness of current filter technologies at blocking access to material that is harmful to minors as defined in the COPA statute?

There is a good deal of circumstantial evidence that filters often fail to block pornography, hate speech, violence, and other forms of content which many filter makers claim to block with 90-95% accuracy. For example a recent study by the Censorware Project (2000) found that 285 Yahoo listed pornography sites (like collegepussy.com) were allowed by at least some of the filter product Bess' proxy servers. In addition, 28 of these sites (like 100analsexpics.com) were fully accessible through all seven of Bess' K-12 school proxies.

A 1997 study conducted by Consumer Reports found that four popular filtering programs failed to block access to at least some of a list of 22 inapropriate web sites. Cyber Patrol failed to block 6 inapropriate sites, CYBERsitter missed 8, Net Nanny missed all 22, and SurfWatch missed 4.

In a study of filter effectiveness in blocking access to alcohol and tobacco web sites, the Center for Media Education concluded that "stand-alone filters do not effectively screen promotional alcohol and tobacco content (1999: 3)."

In my own research efforts, I have attempted to develop a more rigorous methodology for determining filter effectiveness in blocking access to objectionable Internet content. My method combines randomization, multiple web site content samples, and content analysis to determine filter performance. In a recently published study, I found that taken together, four popular filter programs failed to block objectionable Internet content 25% of time (Hunter, 2000). These results have somewhat limited generalizability due to low sample size and the lack of a completely random sample. I have attempted to address these limitations in my "Cyberporn, Filters, and Public Policy: A Content Analysis Research Proposal," which is available for download on the COPA Commission web site. Using my proposed methodology, or one similar to it, I am confident that filter effectiveness in blocking access to objectionable material can be empirically tested. As mentioned in my response to question five, the NAS or NSF would do well to fund non-partisan research along these lines.

10. To what extent do such systems over-filter, that is, also prevent access to harmless material of interest to minors?

There is a tremendous amount of evidence that filter software routinely blocks access to perfectly harmless Internet material. Two groups in particular, the Censorware Project and Peacefire, have extensively documented over-filtering by many of the most popular filter products used today. In a study examining the blocking decisions of SmartFilter in Utah public schools and libraries, the Censorware Project found that the program incorrectly blocked non-objectionable web pages 5% of the time (1999). Among the material that SmartFilter prevented citizens from viewing:

- The Declaration of Independence
- The United States Constitution

- The Bible
- The Book of Mormon
- The Koran
- The Adventures of Sherlock Holmes
- A Connecticut Yankee in Kind Arthur's Court
- George Washington's Farewell Address
- The Mayflower Compact
- All of Shakespeare's plays
- The Canterbury Tales
- Wuthering Heights
- "Marijuana: Facts for Teens" (a U.S. Government brochure)

A similar study by the Censorware Project (1998) found that the X-Stop filtering program used in Loudoun County libraries, unjustly blocked the following non-obscene, non-pornographic, and non-violent web sites:

- The University of Chicago's Fileroom project, which tracks acts of censorship around the world.
- The National Journal of Sexual Orientation Law, which describes itself as devoted to "legal issues affecting lesbians, gay men and bisexuals."
- The Banned Books page at Carnegie Mellon, which gives a historical account of the travails of books such as Candide and Ulysses.
- The American Association of University Women, which describes itself as a national organization that "promotes education and equity for all women and girls."

- The AIDS Quilt site, for people interested in learning more about HIV and AIDS, with statistics on the disease and links to other relevant sites.
- The Heritage Foundation, a conservative thinktank whose mission is to "formulate and promote conservative public policies based on the principles of free enterprise, limited government, individual freedom, traditional American values, and a strong national defense."
- The Religious Society of Friends, better known as the Quakers.
- Quality Resources Online, a clearinghouse for books and other materials relating to quality in business operations.

A recent study by Peacefire found that the I-Gear filtering program incorrectly blocked 74% of sites in the .edu domain under its "pornography" category (2000).

The Gay and Lesbian Alliance Against Defamation (GLAAD) has illustrated through a number of reports that filter makers and access providers including America Online systematically block web sites containing information about the lesbian, gay, bisexual, and transgender community. GLAAD argues that such filtering is particularly harmful for gay teens who often turn to the Internet to help come to terms with their sexuality and to connect with a network of other gay teens struggling with the same issues.

In an April 24th, 2000 article appearing on Cnet's News.com, reporter Brian Livingston uncovered a distinctly conservative bias built into AOL's "youth filters." AOL filters allowed children to view the Republican National Committee home page but not the Democratic National Committee home page. Children could access the conservative Constitution and Libertarian Party web sites, but not those of Ralph Nader's Green Party or Ross Perot's Reform Party. As for gun issue web sites, AOL youth filters allowed access to gun makers Colt and Browning's web sites, as well as the National Rifle Association's page, but denied access to gun control organizations including the Coalition to Stop Gun Violence, Safer Guns Now, and the Million Mom March.

My own research into over-filtering has found that filters incorrectly block benign material 21% of the time (Hunter, 2000). As mentioned in my response to question nine, these results do have limitations which I have attempted to address in a new research proposal. In another study which I concluded earlier this month, I examined the overinclusive filtering of AltaVista's "Family Filter" which is powered by SurfWatch. I conducted two searches with and without Family Filter turned on. My first search was for "gay teens" which resulted in 14,378 unfiltered links compared with just 2 links returned with Family Filter on. I decided to look through the first 20 links on that search and see what types of sites were produced. As would be expected, a number of the sites were pornographic in nature, but 10 of the sites had nothing that would meet SurfWatch's blocking criteria. All ten of these sites (listed in the Appendix) were blocked by the filtered search. AltaVista and SurfWatch are really doing confused teens a service by blocking the "Trevor Project" home page which tries to comfort gay teens contemplating suicide.

The next search I conducted was for "safe sex" which produced 59,118 links with the filter turned off, and a mere 36 with it turned on. Once again I looked at the first 20 links produced by the unfiltered search to see if there were any porn-like pages. The majority were devoted to safe sex and had nothing that SurfWatch should necessarily block. But once the filter was turned on, 11 of these non-objectionable sites were nevertheless blocked (listed in the Appendix). Two blocks are particularly humorous (or sad for that matter). First, Family Filter blocked the Texas ISP Association's (TISPA's) courtesy page for parents seeking information about blocking software. And even better, the filtered search deemed Medicines Sans Frontiers, otherwise known as Doctors Without Borders, the winner of the 1999 Nobel Peace Prize, to be off limits.

While this analysis is less than completely systematic, it does show that filtered search results also exhibit a tendency to over-filter. A more systematic study, including precise rules about search terms, and a content analysis of pages returned by the search engine, would be extremely valuable in gauging the effectiveness of filtered search engines.

11. How many filter systems are in the marketplace, and to what extent do consumers use them?

The GetNetWise web site lists 69 products which filter sexual content. Overall the site lists 129 software tools offering various functionalities to help parents control their childrens Internet use.

Survey evidence indicates that about 30% of parents use some form of filtering software. Refer to my response in question one for a more detailed description of how many parents are using filtering tools, and possible reasons for their relatively low adoption rate.

12. What prevents more widespread adoption of filtering by parents and public facilities, and what can be done to further their use?

A lack of widespread adoption of filter software by parents is likely due to a number of factors. Some parents are unaware of the technology, and others may feel they lack the technical expertise to install and customize the software. In my opinion however, and as outlined in my answer to question one, the biggest reason why parents have not adopted filters is that they trust their childrens online behavior. In addition, many parents have developed simple, non-technical rules about where, when, and how their children can use the net. By solely focusing on ways to promote filter use, we are forgetting to promote a whole host of other techniques which parents are already successfully using to guide their childrens Internet use.

In terms of institutional support for filters, particularly in libraries, greater adoption is hindered by questions about filter effectiveness and by the first amendment implications of the technology. These concerns have been forcefully expressed by the American Library Association in its "Statement on Library Use of Filtering Software" which states:

> Libraries are places of inclusion rather than exclusion. Current blocking/filtering software prevents not only access to what some may consider "objectionable" material, but also blocks information protected by the First Amendment. The result is that legal and useful material will inevitably be blocked. (1997)

While there is a good deal of debate in the library community about the need for filtering software, it would be unwise for the federal government to promote their use until more is known about filter effectiveness and most importantly the constitutionality of filter use in public institutions.

13. How do current labeling and rating systems operate?

The Platform for Internet Content Selection (PICS), developed by the World Wide Web Consortium (W3C) and released in 1996 has become the de facto technical standard for developing rating systems and labeling web content.

The PICS standard basically creates a universal language to describe Internet content. The PICS standard allows for a number of features:

1. The development of numerous rating systems (like RSACi and SafeSurf) to label content along any number of criteria. (the *Rating Services and Rating Systems* protocol)

2. Individual web content providers can select a PICS enabled rating system and voluntarily self-rate their site. (using labels specified by the *PICS Label Distribution Label Syntax and Communication Protocols*)

3. Third parties like the Christian Coalition, or the ACLU can create label bureaus to label sites according to a PICS enabled rating system. (again using the *PICS Label Distribution Label Syntax and Communication Protocols*, but using a different distribution method; a label bureau)

4. Software developers (Netscape, Microsoft, Cyber Patrol, etc.) can use PICSRules to write filters that understand and process PICS-based labels.

5. Verification of label accuracy and source. (the *DSig* protocol)

If a software filter is programmed to interpret PICS labels, it can make blocking decisions based on the description of a web page's content. As mentioned earlier, both Netscape Communicator (in its NetWatch feature) and Microsoft Internet Explorer (via Content Advisor) support PICS-based filtering.

A parent would use PICS to filter a child's access in the following way: Using a PICS compatible filter, the parent selects a trusted rating system, say the MPAA's. The child then begins to surf the web and requests a self-rated site labeled G. The filter grants access to the site because the parent has told it that G rated material is allowable. The child continues to surf, and requests a site that has not self-rated. The filter program then requests a rating of that site (if it is available) from the MPAA's third party label bureau. The MPAA bureau returns an R label for the requested site, and the site is blocked because the filter was configured to deny access to R labeled sites.

This example shows the flexibility of PICS, which allows for both self and third party content rating. On the user's end, the software filter can be programmed to use any PICS enabled rating system. Further, if a requested site is not self-rated, the filter can then request a rating from a third party label bureau. Figure 1 (Resnick, 1998) gives a graphical representation of how a PICS enabled filter might work.

Figure 1: PICS Enabled Client Filter

14. What evidence exists regarding the effectiveness of current labeling technologies at restricting access to material that is harmful to minors as defined in the COPA statute?

Given that a very small percentage of web sites have self-rated their content, it is unlikely that label-based filters are doing much to block access to material deemed harmful to minors. According to RSACi, about 14,400 of the web sites self-rating with their system are rated as inappropriate for children, the vast majority of these being pornography sites (in Mulligan, 1999). If we assume that there are roughly 17 million web sites (Netcraft, 2000), and that 3% of these sites are pornographic in nature (Zimmer and Hunter, 1999), that would mean there are approximately 510,000 pornography related sites. Since RSACi has only been used to rate 14,400 of these sites, pornographic content will not be blocked by label-based filters 97% of the time (unless the filter is set to block access to all unrated web sites in which case it would block 99% of the entire web).

15. To what extent if any do such systems also have the effect of restricting access to harmless material of interest to minors?

As discussed above, for label-based filters to be truly effective they need to block access to all unrated web sites. Since it is quite likely that few non-commercial and individual web developers will decide to self-rate, label-based filters may end up blocking the majority of the web's content, thus reducing the web to a homogenized medium that looks more like cable television than the free wheeling and infinitely diverse resource we enjoy today.

Label-based filters may also end up limiting access to valuable speech because of their over reliance on a particular rating system, and the values it encodes. For example, how should a site dealing with the Holocaust rate itself? RSACi provides four classification categories: violence, nudity, sex, and language. Pictures and content regarding Nazi death camps are likely to contain a good deal of both violence and nudity. However, if a site operator rates this information accordingly, it will likely be blocked by most filters. After all, parents will try to shield their children from sites with excessive nudity and violence. But would parents really want to block access to a Holocaust information web page based on these overly simplistic criteria? As Jonathan Wallace, the creator of a Holocaust information page notes, "ratings systems

404

which lump an Auschwitz Alphabet together with the Hot Nude Women Page ignore this distinction (1996)."

Both ICRA and INCORE are attempting to develop more contextually sensitive rating systems which would allow for artistic and educational exceptions. While this is to be applauded, the more contextual operators included in a rating system, the less reliable the system will become (Weinberg, 1997). This is because people have wildly differing views about what constitutes artistic and educational material. If a rating system can not be applied in a reliable fashion, parents will have no faith in its ability to shield their children from harmful content.

16. How many labeling and rating systems are in the marketplace, and to what extent are web sites labeled or rated?

The two most popular PICS-based rating systems are RSACi and SafeSurf. RSACi claims that about 120,000 web sites have self-rated using the system. Two groups, ICRA and INCORE are currently developing new Internet content rating systems.

17. What prevents more widespread adoption of rating/labeling by web sites, and what can be done to further their adoption?

Diedre Mulligan of the Center for Democracy and Technology nicely summarizes the grim prospect for voluntary market adoption of Internet content rating systems:

> It is doubtful that a new rating system on its own will overcome existing barriers to rating. Those who choose not to rate because

> they engage in activity that is illegal in some country will continue to avoid rating. Web sites where content is a by-product of an underlying activity or interaction are unlikely to rate with an increasingly complex system. Web sites of individual users are likely to remain unrated. It is unclear who will be prompted to rate with the new objective system. If the goal is widespread rating, we fear that it will be unachievable unless rating becomes mandatory. (1999)

And if rating systems become mandatory, they are of course little different than direct government control of speech. I like to call this situation the PICS Paradox. The paradox is that the W3C developed PICS to avoid "global governmental censorship." However, left only to the market, PICS has failed miserably as a protocol. Because few rating systems and rating bureaus have developed, few web sites have self-rated their content. RSACi, by far the most popular rating system, claims that only about 120,000 sites have self-rated using their standard, less than one percent of the web. This shows that on its own, PICS will fail as a market alternative to government action. As such, governments will be incented to step into this vacuum and require that web sites and ISP's self-rate and develop filters using the PICS standard. In other words, the only way for PICS to be widely implemented and used, is if governments, via regulation, require its use. In essence, the W3C's logic behind PICS has been turned on its head. Given the right circumstances, like what is happening in the EU and the Australia, PICS would seem the perfect tool of government censorship, not an alternative to it.

Given the long history of rating systems leading directly to government regulation of speech, and the specific difficulties associated with implementing an Internet content rating system, the federal government should simply leave web developers alone to describe their content in whatever manner they see fit.

References

American Civil Liberties Union. (1998). Censorship in a box: Why blocking software is wrong for public libraries. Available: http://www.aclu.org/issues/cyber/box.html .

American Civil Liberties Union. (1997). Fahrenheit 451.2: Is cyberspace burning? Available: http://www.aclu.org/issues/cyber/burning.html .

American Civil Liberties Union. (1997, 16 July). ACLU wary of White House goals on "voluntary" internet censorship. Available: http://www.aclu.org/news/n071697a.html .

American Library Association. (1997, 1 July). Statement on library use of filtering software. Available via the World Wide Web at http://www.ala.org/alaorg/oif/filt_stm.html .

Bertelsmann Foundation. (1999, September). Self-regulation of internet content. Available: http://www.stiftung.bertelsmann.de/internetcontent/english/download/Memorandum.pdf .

Bertelsmann Foundation. (1999, September). Internet user survey. Available: http://www.stiftung.bertelsmann.de/internetcontent/english/download/Usersurvey.doc .

Censorware Project. (2000). Passing porn, banning the bible: N2H2's Bess in public schools. Available: http://www.censorware.org/reports/bess/ .

Censorware Project (2000). Web size estimates. Available: http://www.censorware.org/web_size/ .

Censorware Project. (1999). Censored internet access in Utah public schools and libraries. Available: http://censorware.org/reports/utah/main.shtml .

Censorware Project. (1998). The X-Stop files: Deja voodo. Available: http://www.censorware.org/reports/x-stop.html .

Center for Media Education. (1999). Youth access to alcohol and tobacco web marketing: The Filtering and rating debate. Available: http://www.cme.org/ .

Consumer Reports. (1997, May). Children online report. Consumer Reports, Vol. 62 (5), 27.

Cyveillance. (2000). Size of the internet. Available: http://www.cyveillance.com/ .

Davison, W.P. (1983). The third-person effect in communication. Public Opinion Quarterly, 47.

Hunter, C.D. (2000, Summer). Internet filter effectiveness: Testing over and underinclusive blocking decisions of four popular filters. Social Science Computer Review, Vol. 18 (2), 214-222.

IDC. (1999). Web-site globalization. An IDC White Paper. Available: http://www.etranslate.com/en/about/IDCglobal.pdf .

Johnson, D., and Post, D. (1996). Law and borders: The rise of law in cyberspace. Stanford Law Review, 48: 1369-76.

Kaiser Family Foundation. (1999, May). Parents and the V-chip. A Kaiser Family Foundation Report. Available: http://www.kff.org/ .

Kendrick, W. (1987). The Secret museum: Pornography in modern culture. New York: Viking.

Kubota, G. (1997). Public school usage of internet filtering software: Book banning reincarnated? Loyola of Los Angeles Entertainment Law Journal, 17.

Lasica, J. (1997, 31 July). Ratings today, censorship tomorrow. Salon. Available: http://www.salonmagazine.com/july97/21st/ratings970731.html .

Livingston, B. (2000, 24 April). AOL's "youth filters" protect kids from Democrats. News.com. Available: http://www.news.com/Perspectives/Column/0,176,421,00.html .

Mainstream Loudoun, et. al. v. Board of Trustees of the Loudoun County Library. (1998). Civil Action No. 97-2049-A. Available: http://www.aclu.org/court/loudounvboard_dec.html .

Mulligan, D. (1999, October). An analysis of the Bertelsmann Foundation memorandum on self-regulation of internet content. Center for Democracy and Technology. Available: http://www.cdt.org/speech/991021bertelsmannmemo.shtml .

Netcraft. (2000, June). Netcraft web server survey. Available: http://www.netcraft.com/survey/ .

NUA. (1999, 29 March). Techserver: Internationalisation of the web. Available: http://www.nua.net/surveys/?f=VS&art_id=905354800&rel=true .

Peacefire. (2000). IGDecode: I-Gear list codebreaker. Available: http://peacefire.org/censorware/I-Gear/igdecode/ .

Resnick, P. (1998, 26 January). PICS, censorship, & intellectual freedom faq. World Wide Web Consortium. Available: http://www.w3.org/PICS/PICS-FAQ-980126 .

Roberts, D. (1996, 28 August). Media content rating systems. The Wally Langenschmidt Memorial Lecture. Available: http://www.rsac.org/ .

SafeSurf. (1997). Online cooperative publishing act. Available: http://www.safesurf.com/online.htm .

Smolla, R. (1997, Summer). The Culture of regulation. CommLaw Conspectus, 193.

Strossen, N. (1999, September). Comments of Nadine Strossen. Available: http://www.aclu.org/issues/cyber/strossen_munich.html .

Taylor, P. (1999, 3 September). Senator defends entertainment-labeling as 'citizenship,' not censorship. Free!. Available: http://www.freedomforum.org/ .

Taylor, P. (1998). Lawmakers, citizens groups step up efforts to monitor entertainment industry. Free!. Available: http://www.freedomforum.org/ .

Turow, J. and Nir, L. (2000). The Internet and the family 2000: The View from parents the view from kids. Annenberg Public Policy Center of the University of Pennsylvania, Report No. 33. Available: http://appcpenn.org/finalrepor_fam.pdf .

Turow, J. (1999, May). The Internet and the family: The View from parents the view from the press. Annenberg Public Policy Center of the University of Pennsylvania, Report No. 27. Available: http://www.appcpenn.org/internet/ .

Wallace, J. (1997). Purchase of blocking software by public libraries is unconstitutional. Briefing Paper. Available: http://www.spectacle.org/cs/library.html .

Wallace, J. (1997). Why I will not rate my site. The Ethical Spectacle. Available: http://www.spectacle.org/cda/rate.html .

Weinberg, J. (1997). Rating the net. Hastings Communication & Entertainment Law Journal, 19, 453.

Woodard, E. (2000, June). Media in the home 2000. Annenberg Public Policy Center of the University of Pennsylvania. Available: http://www.appcpenn.org/inhome.pdf .

Zimmer, E. and Hunter, C.D. (1999). Risk and the internet: Perception and reality. Presented at the Citizens at the Crossroads Conference, New London Ontario, October 1999.

Appendix: AltaVista Family Filter Test

All searches were conducted on July 7, 2000.

AltaVista Search - "gay teens"

14,378 filter off
2 filter on

Sites with no blockable criteria that were nevertheless blocked (among first 20 links produced by unfiltered AltaVista search):

http://www.angelfire.com/ns/gts/menu.html
GAY TEENS @ SINGAPORE HOMEPAGE

http://www.cnn.com/US/9910/23/gay.violence.summit.02/index.html
CNN article about falwell summit

http://www.advocate.com/
The national gay & lesbian newsmagazine Internet site

http://www.youthresource.com/
Gay youth resource site

http://members.spree.com/usagi987/gay.htm
Gay youth links to support groups

http://www.trevorproject.com/
suicide prevention for gay youth

http://www.iwannaknow.org/
Gay teen portal

http://www.armory.com/~web/gaybooks.html
Gay and Lesbian Characters and Themes in Children's Books

http://www.temenos.net/
Gay Portal

http://www.wired.com/news/topstories/0,1287,9284,00.html
Wired News article about gay web sites

AltaVista Search - "safe sex"
59,118 filter off
36 filter on

Sites with no blockable criteria that were nevertheless blocked (among first 20 links produced by unfiltered AltaVista search):

http://www.cnn.com/HEALTH/9810/02/moms.condoms/
CNN news story about moms talking with children about safe sex

http://www.detnews.com/menu/stories/42593.htm
Detroit News article reporting that safe sex reduces the chances of cervical cancer

http://www.y2ksafesex.com/
empty domain advertisement, one picture of a condom

http://www.traveltomuskoka.com/
Travel promotion page with one link to safe sex page

http://www.rubbertree.org/
The Rubber Tree condom store

http://www.winstonsmith.com/gallery/book1/small/safe2.html
Art gallery poster

http://www.quickcondoms.com/
Condom store

http://www.tispa.org/filtering.htm
Texas ISP Association's (TISPA's) courtesy page for parents seeking information about blocking software

http://www.msf.org/
Medicines Sans Frontiers otherwise known as Doctors Without Borders, the winner of the 1999 Nobel Peace Prize.

http://www.studentadvantage.com/health
Student Advantage health page

http://www.shophustler.com/safesex.html
Hustler page, but has nothing more than a statement on safe sex

Biography

Zachary Britton

Zachary Britton authored the book "Safety Net: Guiding and Guarding Your Children on the Internet," along with many articles on Internet safety. He has also been a guest on many television and radio programs dealing with Internet issues. As part of his online safety research, Mr. Britton has tested many server and client side filtering products to review their relative efficacy.

Mr. Britton is the cofounder and Chief Executive Officer of Front Porch Communications (FPC). Mr. Britton has several patents pending on technologies used by FPC to provide anonymous profiling and content distribution services to over 100 ISPs located in 11 countries.

Mr. Britton has over ten years of professional online experience. He was previously the Chief Executive Officer of International Business Simulations, Inc., a firm specializing in online executive education tools. He was instrumental in the development of the first Internet-based, "business simulation" training program, IB SIM, which has been used successfully as a learning tool in corporations and universities worldwide, including the Graduate School of Business at Harvard University and the Anderson Graduate School of Management at the University of California, Los Angeles.

In addition to the prior mentioned endeavors, Mr. Britton built, managed and sold his own regional ISP, which enjoyed dynamic growth and sustained profitability under his leadership.

Mr. Britton holds a Master of Arts Degree in International Management and Policy

KAREN G. SCHNEIDER

EDUCATION

1992 University of Illinois, Urbana, IL
M.S., Library and Information Science

1982 Barnard College, New York, NY
B.A., English

LIBRARY EXPERIENCE

1999 - Director of Technology, Shenendehowa Library
Clifton Park, NY
Director of Technology

- Leads the technology effort for a well-respected public library serving 50,000
- Introduced web databases, remote database access, staff training, and e-books
- Created and leads first consortium-wide technology advisory group
- Provides hands-on support of NT Server and related applications
- De facto director of staff training, helping staff update software and hardware skills through one-on-one, in-house and commercial training opportunities

1998 - 1999 Brunswick Community Library
Brunswick, NY
Director

- Automated small-town library from the ground up in 14 months
- Introduced remote database access, public Internet training

1996 - 1998 Garcia Consulting, Inc.
New York, NY
Director, U.S. EPA Region 2 New York Library

- Turned little-used eyesore into highly-regarded flagship division
- Led successful migration to Internet-accessible commercial databases
- Key indicators (reference, circulation, ILL, traffic) up every quarter

1994 - 1996 Blue Highways
Wayne, NJ
CEO

- Ran successful Internet training business for 18 months
- Wrote and taught curriculum, traveled to new sites

1993 - 1994 Newark Public Library
Newark, NJ
Electronic Resources Librarian

- Science and business reference for busy urban library
- Helped write successful national telecommunications grant

1992 - 1993 Queens Borough Public Library
Jamaica, NY
Children's Librarian/Electronic Resources Librarian

298 South Main Avenue, Albany NY 12208 | kgs@bluehighways.com | voice 518-437-0664

- Hand-picked to help bring Internet on board; developed training services

More information on page 2...

OTHER SIGNIFICANT WORK EXPERIENCE

1983 - 1991 United States Air Force
Worldwide
Aircraft maintenance specialist. Highest rank: captain

- Engine mechanic, later commissioned as maintenance officer
- Served five tours, three overseas
- Responsible for hundreds of personnel, billions of dollars of equipment

INTERNSHIPS AND ASSISTANTSHIPS

1991 - 1992 Graduate Library, University of Illinois
Urbana, IL
Graduate Assistant

- Reference services, instruction and online searching for a 35,000-member population

AWARDS AND HONORS

- 1998 Leadership Award, University of Illinois Graduate School of Library and Information Science
- Best article of the year, The Bottom Line, 1998
- Air Force Commendation Medal with three oak leaf clusters
- Selected by Electronic Frontier Foundation in 2000 to accept Pioneer Award for librarians everywhere on behalf of our profession's support for intellectual freedom

COMMUNITY ACTIVITIES

- Project Leader, The Internet Filter Assessment Project, 1997. Led librarian-organized project to assess Internet content filters
- Frequent speaker to library organizations
- Created first Website for Episcopal Diocese of Newark

PROFESSIONAL INVOLVEMENT

- Councilmember-at-large, American Library Association, 1997 - 2000.
- Co-moderator, PUBLIB, discussion list for public librarians, 1996 - .
- Chair, ALA Electronic Meeting Task Force, 1999 - .
- Member, ALA Committee on Research and Statistics, 1999 - .
- Founding member, New Jersey Library Assocation Gay and Lesbian Roundtable
- Member and active participant, LITA Internet Room Committee, 1993 – 1996
- Adjunct instructor, School of Information Science and Policy, SUNY Albany

PUBLICATIONS (A SAMPLING)

Books

BEST COPY AVAILABLE

The Internet Access Cookbook, Neal Schuman, 1996

Articles

Column: The Internet Librarian, June 1995 – , *American Libraries*

The Tao of Internet Costs, *The Bottom Line, Spring 1998*

References on

Testimony of Karen G. Schneider

Before the

COPA Commission

Internet Content Filtering In Libraries:

The Wrong Tool For The Wrong Job

July 20, 2000

Karen G. Schneider
Assistant Director for Technology
Shenendehowa Public Library
Clifton Park, NY 12065
518-371-8622
she_schne@sals.edu

Ms. Schneider is a library administrator at Shenendehowa Public Library in Clifton Park, New York, a library serving approximately 50,000 patrons. Her specialty is library technology, and her responsibilities including maintaining the Local Area Network, supervising the automation division, managing staff training, and technology planning. Her library career path includes a directorship of a small public library, electronic services, children's library services, and running a one-person Internet training business. Before her library career, Ms. Schneider was an aircraft maintenance officer in the U.S. Air Force.

Ms. Schneider is also a columnist for American Libraries and has published two books, most notably A Practical Guide to Internet Filters (Neal Schuman, 1997). In 1997, she led a team of librarians in an informal study of Internet content filters, and in 1998 was an expert witness for the community group Mainstream Loudoun citizens' group in the case, Mainstream Loudoun vs. Board of Trustees. Her article, "The Tao of Internet Costs," was selected for the 1999 Award of Excellence by the library finance journal, The Bottom Line. She is a frequent speaker at library conferences and since 1998 has been an adjunct instructor at the School of Information Science and Policy at SUNY Albany, where she has taught Internet access issues and introductory web design. In 1998, Ms. Schneider was elected to the Council of the American Library Association, and she chairs the American Library Association Task Force on Electronic Meeting Participation. Since 1996, Ms. Schneider has co-moderated PUBLIB, an electronic discussion list for public librarians with over 4,000 subscribers.

Mr. Chairman and Members of the Commission. Thank you for this opportunity to present information to the Commission on these important issues. My testimony reflects only my own views on the issues; I am not testifying on behalf of any organization.

I have been asked to survey the general characteristics and/or policy implications of the Internet content technologies with which I am most familiar. In this testimony I address the effectiveness of Internet content filtering technologies, the prevalence of filtering technologies, and legal and policy concerns. My primary focus will be on filtering in the context of the world I know best: public libraries.

The Commission has posed excellent questions; all of these issues are closely interrelated. In particular, the questions about the effectiveness of filtering and the prevalence of filtering go hand-in-hand.

Available Filtering Methods

Filtering methods that actually exist as of this writing are filtering by blocking sites and keywords, "family-friendly" search engines, and rating tools such as PICS.[1] Most of these tools rely on stoplists or go-lists maintained by third-party providers. In most cases, stoplists, or lists of sites that filters prevent access to, are encrypted and cannot be viewed by the licensor or the end-user. Other features include "rules-based" filtering, in which filters use algorithms to calculate on-the-fly whether a page should be viewed, and, common to nearly all filters, categories, in which the licensor or software administrator may select the areas to be blocked. Finally, some filters, particularly proxy-based filters, provide the ability to tailor filtering based on machine or user account status. So, for example, all computers in a public area could be blocked from accessing a category described as "alternative lifestyles," while computers in the system administrator's area could access all Internet content.

Filtering Methods that are Not Available

Other tools frequently discussed, but unavailable in anything but prototype versions, include tools for examining graphic pixels, fuzzy-match, and similar attempts at advanced content analysis. Tools that this author has not evaluated in several years include filtering software that works on interactive tools such as chat/IRC, Instant Message, and email. (All filters have the capability to block chat- or mail-specific websites, however, and many libraries do not offer Instant Message or related tools or allow patrons to install them on public computers.)

Have Filters Changed?

In 1997, I provided reviews of one dozen Internet content filters in my book, A Practical Guide to Internet Filters. I included detailed descriptions of how filters work, discussions of individual products, criteria for assessing Internet content filters, and discussions of real-world decisions made by libraries that chose to filter or not filter.

Since 1997 I have evaluated filters on a quarterly basis or more frequently as the need arose, and I have kept current in computer-related literature. Most recently I have evaluated I-Gear, from Symantec, and Elron Internet Manager. Despite new features and new product claims, to the best of my knowledge, there have been no advances in Internet content filtering technology that change any of my earlier conclusions; this is not surprising, given that forty years of information-science research into artificial intelligence still leaves us far short of any dramatic breakthroughs. Generally, in my analyses of filtering products, I have found that "new" features touted as "breakthroughs" tend to be elaborations on dynamic algorithm generation, and have the same relationship to artificial intelligence as earthworms do to primate intelligence.

How Filters Work: A Task Analysis

With all the discussion of Internet content filtering, it is beneficial to step through a task analysis of installing filters in a working environment to understand the characteristics of the products we are discussing. The environment selected, again, is the public library, where an end-user sits down at a public-access computer.

1. The filtering company creates, markets and sells the Internet content filters as well as the stoplists included in the filter.
2. Filtering software is purchased and installed.
    a. May be installed on a client (an individual workstation) or a server.
    b. May be used for all or some of the computers in a library, or all or some of the library accounts.
3. The administrator of the filtering software determines which filtering categories should be enabled.
    a. Actual content of these categories is unavailable to the administrator or the end-user.
4. The administrator enables the filter.
5. May be enabled in all circumstances, or for specific accounts, computers, or time of day, or for specific patron access (adult or child).
6. The end-user starts an Internet session.
    a. The entire Internet session may be considered to be interpreted through the content filter.
    b. The end-user may or may not be presented with an Internet policy statement, may or may not be aware that a filter is installed, and may or may not be able to choose whether the filter is enabled.

    c. The end-user does not control or have access to the stop-lists, and may not be aware that filters function through stop-lists, and will not know what is included in the stoplists.

7. The end-user performs a search.
    a. If the site is not blocked by the filter, the site is displayed.
    b. If the site is blocked by the filter (statically or dynamically, through keyword or site blocking, with or without algorithms), the site is not displayed.
8. If the site is blocked, a message may or may not appear informing the end-user that the site is blocked; this is a "denial page." In some cases the denial page may be customized, and may include an email link for requesting more information about the block. Other information that may be provided on the denial page includes:
    a. A picture of a dog saying "Bess doesn't want you to go there"
    b. An error message, such as "Cyber Patrol Code 2" or "access denied"
    c. A return to the previous search page, or to the main search page
    d. Information about the blocked site, including URL, time blocked, and the filter's category for blocking the site.
9. The content-provider is not notified at any point that an end-user has been or will be denied access to the site.
10. A patron who sees a denial page or otherwise believes that a site may be blocked has several options, including the following:
    a. If the patron has been guided to do so, the patron may email the library or the filtering company to request more information about the blocked site.
    b. If the patron has been guided to do so, the patron may locate a library employee and request in writing or orally for more information about the blocked site.
    c. The patron may ignore the message and continue searching.

Observations Based On The Task Analysis

In the task analysis above, there are a breathtaking number of opportunities for censorship of protected speech and viewpoint discrimination—intentional or otherwise. First, the filtering company—a commercial third party with no obligations or motivations for safeguarding free expression--not only decides which sites to block, but creates categories for site-blocking that go far beyond anything that is arguably illegal content, including categories such as "questionable" and "militant"—areas that certainly will offend some people but are not illegal. The filtering company establishes itself as the library by proxy, stepping in to create content decisions while simultaneously hiding that information from the library or the library patron. The library must then play a role in selecting the Internet content filter, deciding which categories to block, and other conditions (time of day, workstation, user, etc.).

The patron may or may not be aware that his or her search is filtered, and in most cases is not aware of which categories were blocked, why the library selected those categories, or the criteria of these categories as established by the filtering company. The patron is probably unaware that—unlike other resources in the library—the library staff had no way to access to the content of the stoplists (and, as described later, would face legal action if they attempted to determine the content). In the event that a site is filtered, the patron may be confronted with an obscure, misleading, or off-putting message, similar to "404 Not Found" messages indicating broken links. In the event that a patron sees a message providing a means to inform the library staff or the filtering company, the burden is still on the patron to decide to report the incident and follow through on the library's or filtering company's decision.

Finally, the content provider is left completely in the cold, unaware, in the fog and friction of filtering, that their content was targeted for blocking, and unaware that a potential reader was denied access.

The Question of Effectiveness

Only within this task analysis is it meaningful to discuss the "effectiveness" of Internet content filters. In 1997, I spent six months exploring filtering "effectiveness" when I led The Internet Filter Assessment Project, a team-based study of site and keyword blocking filters in which three dozen librarians participated. Though this project was informal and unscientific, the process of examining Internet content filters, including the time spent evaluating a wide variety of over a dozen Internet content filters and the collection of over 1,000 survey forms, led to a series of valuable conclusions about filtering technology. Some of the findings were:

- Filters are inconsistent in what they block
- All filters block some information that project participants felt should not have been blocked
- Project participants did not agree among themselves on the nature of "appropriate" versus "inappropriate" content"

These findings are naturally related, and lead to a larger "meta-finding" about filtering effectiveness: All Internet content filtering technologies, including those that claim to be "advanced," "third-generation," or otherwise "new and improved," have a fatal flaw that cannot be overcome by technical wizardry: they are mechanical tools wrapped around subjective judgment. Though tools used to scan the Internet for new websites, measure images for instances of suspect pixels, or screen live content dynamically are undeniably sophisticated in the most literal sense, on another level, these tools are hopelessly naïve, because they are entirely dependent on human decisions to determine whether information is or is not "appropriate." In this sense, the "effectiveness" of an Internet content filter is always self-referential; it only refers to how well the filter performed based on the arbitrary decisions of the humans who selected the material others would not see.

Furthermore, the "effectiveness" of Internet content filters is intentionally hidden from public view by filter companies, who aggressively guard this content. Earlier this year, two computer enthusiasts cracked the code for the stoplists of Cyber Patrol and published the formula for decoding the filter stoplists. Tellingly, for several years websites such as Peacefire have provided instructions for disabling Internet content filters, which have elicited corporate grumbling from filtering companies, yet it took the publication of a rule for revealing the content of blocked sites to arouse true ire from Mattel, Cyber Patrol's owning company (suggesting also that the company's priorities are market-driven, not oriented toward "protecting" children or other users). Not only were the two hackers threatened into silence, but anyone who mirrored the content of their website was vulnerable to legal action. Cyber Patrol now explicitly states that it blocks all websites that provide information about "hacking" Cyber Patrol.[iii]

The Arbitrary Nature of Filtering Stoplists

Logic would suggest that if filter stoplists were irrefutably objective and reliable—that if, in other words, the nature of websites could be evaluated as scientifically as how accurately a spreadsheet performs a mathematical equation—then the stoplist information would be low-value data, shared by all companies and publicly available, and that the fiercely-guarded secrets would be instead the value-added qualities of the respective filters, much as Lotus and Microsoft do battle over spreadsheet features rather than the ability to add or divide within a cell. The Cyber Patrol case proves that the opposite is true: Internet content filter companies claim that stoplists are highly valuable corporate information due to their unique nature, and must be protected at all costs. In other words, there is no immutable body of agreed-on data that all companies agree must be filtered at all times by all products.[iv]

What does Cyber Patrol (or any other filtering company) have to hide? It is probable that most filtering companies do not have intentional agendas for viewpoint discrimination. Instead, the primary motive for filtering companies—and of itself, of course, there is nothing wrong with this--is commercial. The major selling point of an Internet content filter is its perceived "effectiveness"—how well (and how specifically) it blocks Internet content. Critics of filtering get the widest media coverage, not by pointing out the more nuanced issues related to filtering, but by emphasizing the spectacularly obvious errors some filters have made—blocking sites such as the Quakers, the American Association of University Women, and so forth.[v] As a company, Cyber Patrol can prevent discussion of which sites it blocks, and bolster it position in the filtering marketplace, by immuring its mistakes in an encrypted database, where no one can mock a company that in the name of "online safety" prevents access to a college quilting club.[vi]

An equally important (and related) reason to keep stoplists hidden is because it creates the illusion of a seamless body of "harmful," "illegal," "inappropriate," "offensive" material usually labeled as "porn," "child pornography," or "dangerous material"—even though a study by Burt showed that 15% of one filter's blocks were sites that were "non-sexual," "undeterminable," or "dead links," and to Burt, this was an *effective* filter.[viii] The "seamless body" perception is important to minimizing discussion and debate about the nature of Internet content filtering.

This brings us again to the highly subjective nature of Internet content filtering, the complexity of introducing this filtering into a computing environment where only one of the stakeholders (the content filter company) has information or control over the information being blocked, and ultimately to the inability of filters to reflect community standards.

Several documents submitted to the COPA Commission dispute whether or not specific websites should have been blocked by filters. In my second expert report submitted for the Mainstream Loudoun trial, I argued that a gay-themed jewelry site should not be blocked; Mr. Burt argued that it should be blocked because its hosting site was "porn" (though he did not explain why the jewelry site fit into that category).[viii] This common filtering debate is the most telling symptom that Internet content filters are simple mirrors of individual attitudes and mores. As I discovered in The Internet Filter Assessment Project, the most important variable in determining whether a specific website "should" be blocked was the person making the decision. TIFAP selectors had their own internal consistency, but ranged widely in their attitudes about material, particularly content that could be construed as controversial.

A Shoebox Fit for Community Standards

Mr. Corn-Revere, in his testimony to the Commission on June 8, observed, "It is not surprising…that different communities will have very different views on what information might be deemed 'harmful to minors.'"[ix] The question of variable community standards creates another "effectiveness" issue with respect to Internet filters. What is a "community standard" for a software product developed and maintained by a small team of individuals in Boston, Austin, or Seattle? How can an Internet filter customize itself automatically to the mores of a local community (let alone an individual reader)? The answer, of course, is that it cannot. This is likely why filtering is not widely adopted by libraries, and that of these libraries, the majority will tell you that they are filtering in response to political pressure, not out of any belief that filters create an Internet environment customized to the communities, let alone the individuals who make up these communities. A filter that claims to meet all community standards is probably blocking so broadly that it cannot be accused of inattention. Again, the hidden nature of the blocked information complicates matters, because many naïve users may easily assume that the filter is "effective" in the sense that it is blocking out only the "bad stuff" as *they* understand it.

Filters And The Presumption of Prurience

An expression created during The Internet Filter Assessment Project was "the presumption of prurience," which refers to the presumption implicit in the design of filters (most likely an outcome of the crudeness of the product) that controversial, potentially offensive, and sexually explicit content (as determined by the filtering company) should be blocked without any consideration of the intentions of the reader. The phenomenon of "the presumption of prurience" is closely related to the problem with community standards; it is expecting far too much of a software program for it to anticipate the intent or the reaction of the end-user. It is impossible to distinguish among a patron who is simply curious, one who is seeking sexual gratification, or someone, like Mr. Burt, who claims to have viewed hundreds of "porn" sites in the name of protecting children.

"Community" or Market-Driven Standards?

Finally, the effectiveness of a software product can be driven very heavily by how much you believe you can trust it to perform predictably. Because filters are software driven by viewpoint decisions made by humans, they are vulnerable to the same human failings we find wherever human judgement is involved, and that can make them highly unpredictable.

Project Bait and Switch, from the Peacefire organization, revealed that filtering can be a conduit for highly nuanced, subjective, possibly market-driven decisions.[8] Peacefire, an advocacy group for youth access to the Internet, sent anonymous submissions to filtering companies asking them to block identical material they claimed was, respectively, from small, free websites maintained by individuals and from large, established websites from well-known organizations such as Focus on the Family. Project Bait and Switch showed that filtering companies will block material on free home pages (in this case, anti-gay propaganda) that they will not block when it appears on the home pages of more well-known, well-funded groups. Filtering companies, like all of us, are attuned to notion that larger entities have more political and financial power. The outcome, sadly, is that different standards of access prevail for different content providers. In this sense, filters are ineffective because they cannot be trusted to be neutral to the source of the content.[xi]

Comparative Effectiveness of Filtering Versus Policy

For a filter to be "effective," it must have a problem to resolve. It is safe to say that all libraries in the United States have bodies of policy and procedure for managing library use. It is also a safe generalization that most library policies are about the many activities in libraries that are not about public Internet use. Many library policies and procedures have been developed in anticipation of, or in response to, exceptional behavior by library users.

Internet policies help libraries tailor their response to Internet use according to community behavior as well as to how the community expects the library to communicate with their patrons. Many times, these policies reflect lessons learned in other areas of librarianship. A library with high-traffic computer use and limited machines might impose strict time limits. A library where many patrons do not have access to computers anywhere else may even encourage use of interactive tools, such as web-based email, or require introductory courses on Internet use.

Identifying The Target Problem

If we are considering the effectiveness of Internet content filters, it is important to understand the nature of the problem we are purportedly addressing with these tools. Are we are talking about a widespread human phenomenon of justifiable social concern, or routine, even predictable patterns of misbehavior by a small number of miscreants? The facts are that patron misuse of the Internet is highly consistent with other library misbehavior: a miniscule percentage of the patrons cause the majority of the problems, which themselves are very small in comparison to total library activity.[xii] (We are also assuming, for the moment, that "problems" include the retrieval of Internet sites that may not be problems at all, depending on who is making the determination.)

In evaluating Internet content filter log files, Burt, whose assessment of what he construes to be "porn" is by his own admission very broad, still only found that between one-half and one-third of one percent of all Internet access was blocked by Internet filters, yet he justifies his concerns by claiming that each blocked site translates, in his words, into "thousands of separate incidents."[xiii] He contradicts himself later when he reports an instance where one sexually-explicit website was accessed 225 times, then notes that "the most likely conclusion is that all 225 attempts were made by a lone individual…"[xiv]

The notion of the "bad actor patron" is not only consistent with current patterns of library behavior, but is also consistent with anecdotal reports from librarians, as well as stories in the media, which focus on cases where one individual accessed information deemed inappropriate for a public environment. In fact, most of the "testimony" on the defunct website, www.filteringfacts.org, focuses on isolated incidents involving situations where one person *saw* another person *viewing* something that the first person felt was inappropriate or objectionable. The reality of the "bad actor patron" is another reason why statements about the number of library users who are accessing material that may be harmful to minors should be evaluated carefully. Burt, for example, claims that at one library there were over 4,000 "separate incidents," but he means that there were by his estimate 4,279 blocked sites that he "assumes" were sexually-explicit to the point where he, Burt, would expect them to be blocked, and which realistically were probably accessed in far fewer than 4,000 sessions. Furthermore, this library reported over 14 million websites accessed during this same period. 4,000 websites may seem like an enormous number—but within the context of total public use, dwindles to a pittance.

Similarly, Crystal Roberts, of the Family Research Council, attempts to persuade the reader of a major and pernicious problem at Los Angeles Public Library, by citing 7 adults who claim to view "porn" a lot, 2 children known to have accessed (adult) sexually-explicit sites, and a "handful" of additional (vaguely referenced) adults. Yet LAPL is one of the highest-traffic libraries in the country. As a librarian who has worked in poor urban areas—Jamaica, Queens and Newark, New Jersey—a day where only 9 to a dozen patrons misbehaved seems like a vacation. To place this in even larger context, there are an estimated 122,440 libraries in the United States; Ohio alone has over 7.5 million registered users. Within the scope of possible human behavior, and the degree to which Americans use their libraries, the single-digit reports of problem behavior seem trivial indeed.

The evidence—however anecdotal, or deduced from other known library patron behavior—that a small number of library patrons comprise the vast majority of the accesses for sexually-explicit websites puts a very different spin on Burt's conclusions in Dangerous Access. It is a different management problem, and it raises the question whether, given the known deficiencies of filters, filtering all patrons, all the time, is the most effective tool for managing Internet access. If most patrons, most of the time, do not access content that is illegal, let alone merely objectionable—and the projections range from 99.5% to 95% of "good" behavior even by stringent standards of filtering proponents such as Burt—then filtering all computers, or most computers, in a public environment, appears to be an inappropriately draconian response to a library management problem which, compared to book theft and loss, cell phone abuse, general rambunctiousness of adolescents, and true criminal activity, is of Lilliputian proportions.

Privacy Buffer Zones and the Inadequacy of Internet Filters

When we step away from debating the proxy-server log files and whether a site is "porn," some other observations are possible. One is that Internet content filters do nothing to address the very serious problem created by public-access computers: the significant erosion of the "privacy buffer zone," which is what I call the invisible bubble of privacy around a patron engaged in classic book-based reading behavior. Only a few extreme groups believe that people are not entitled to read what they want to read in public libraries.[xvii] Regardless of what libraries purchase, we do not ransack briefcases or backpacks to ensure that patrons' own reading materials conform to "community standards" or our personal sense of appropriateness, nor do we police reading tables, peering over shoulders to spy on what people are reading. Yet in many public libraries, patrons must conduct all of their electronic explorations in full view of librarians, other patrons, including children, and the people sitting next to them. You cannot carry a computer to a private cubicle to look up information about divorce, cancer, or vasectomies. Not only that, while most adult fiction contains a soupcon of titillation, the reader who seeks even the mildest equivalent material on the Internet may soon feel awkward and uncomfortable. If the viewer is comfortable enough to view this content in public, then someone will undoubtedly walk by who feels that his or her privacy boundaries have been violated, and may well object indignantly at being "exposed" to "porn" even as he or she carries out an armful of material laden with salacious moments.

Both the reader and the passer-by have equally valid claims to that very important right—the right to be left alone: left alone to read in peace, left alone to traverse through society without being exposed to too much noise, pollution, ozone, or computer-generated images. In fact, many incidents in libraries are about what happens when these rights are violated. Internet content filters do not address the issue of ensuring access to Constitutionally-protected speech while ensuring the right to privacy. All filters can do is prevent these situations by denying the viewer access to material he or she seeks out.

Conclusion

There have been extensive and spirited debates about the quantity of Constitutionally-protected speech that is blocked by Internet content filters. However, no one denies that Internet content filters block access to protected speech. To the extent that libraries are the town squares for the free marketplace of ideas, Internet content filters are ineffective, in that they are guaranteed to block information people have a right to access, and to block it in such a way as to equally and stealthily harm the provider and the reader. The question is not whether the amount of speech blocked by Internet content filters can be reduced to an acceptable minimum. The question is how to use the tools we have, such as policy and education, to further free speech in an open society.

---

[i] For an extended discussion of filtering technologies, see Schneider, Karen G. A Practical Guide to Internet Filters. New York: Neal-Schuman, 1997.

[ii] Schneider et al. The Internet Filter Assessment Project (1997). http://www.bluehighways.com/tifap

[iii] See http://www.cyberpatrol.com/cybernot/criteria.htm

[iv] For an example of how a filtering company "allows" users to request sites be blocked or unblocked, see the Cyber Patrol Appeals Process (July 15, 2000). http://www.cyberpatrol.com/cybernot/appeals.htm

[v] See, for example, the original Mainstream Loudoun complaint, at http://www.censorware.org/legal/loudoun/971222_complaint_ml.htm

[vi] McCullagh, Declan (2000). http://www.politechbot.com/p-00995.html

[vii] Burt (2000). Dangerous Access. Archived in several places, including www.filteringfacts.org. P. 40ff.

[viii] Expert reports of Schneider and Burt are available online at http://www.censorware.org/legal/loudoun/

[ix] Corn-Revere, Robert (2000). Legal and Policy Implications of "Cyberzoning." Unpublished. [COPA Commission.]

[x] Peacefire (2000). http://www.peacefire.org/BaitAndSwitch/

[xi] See also McCullagh, http://www.wired.com/news/politics/0,1283,36621,00.html

[xii] For an extensive bibliography on crime in libraries, see Pease, Barbara (1995). Workplace Violence in Libraries. Library Management, v. 16 n. 7, pp. 30-39.

[xiii] Burt (2000). P. 44

[xiv] Burt (2000). P. 44

[xv] Burt (2000). P. 43ff

[xvi] Burt (2000). 40ff

[xvii] All of which support filtering; e.g. Family Friendly Libraries, www.fflibraries.org

David Burt

Software Tester, Competitive Intelligence Department N2H2, Inc.

David Burt is currently employed as a software tester and competitive intelligence specialist at a N2H2, a leading Internet infrastructure company specializing in filtering, Internet management and content delivery services. Much of Mr. Burt's work for N2H2 involves the in-depth analysis and testing of Internet content management products. Mr. Burt joined N2H2 this year after nearly three years as president of Filtering Facts, an organization devoted to the study and promotion of Internet content management software.

Mr. Burt is recognized as a leading expert on Internet content management, having evaluated filtering products for such publications as the New York Times and the Dr. Laura Perspective Magazine. Mr. Burt has frequently provided expert testimony on the effectiveness of filtering software, having testified before the National Commission on Library and Information Science, in the case Mainstream Loudoun v. Board of Trustees, and before the Pennsylvania State Legislature.

Mr. Burt has also been the subject of frequent news stories detailing his activities to promote filtering software, in such publications as the New York Times, the Wall Street Journal, USA Today, the San Francisco Chronicle, the San Jose Mercury, the Associated Press, and the Chronicle of Higher Education.

Mr. Burt possesses a Masters degree in Library and Information Science from the University of Washington, and is a former librarian. In his previous employment at the Lake Oswego (OR) Public Library, Mr. Burt oversaw a network of computers that included public Internet stations equipped with Internet content management software.

Written Testimony of David Burt
Child Online Protection Act Commission
July 20, 2000

I) Introduction

Thank you for allowing me this opportunity to submit testimony to the Commission on Child Online Protection. In my testimony I will discuss the current state of Internet content management (ICM) technologies, how ICM technology works, the evidence gathered to date regarding the effectiveness of ICM technology, and a proposal for further study.

II) History and current state of Internet content management technology

Internet content management technology, sometimes referred to as "filtering software" or "blocking software", first appeared commercially in 1994. ICM software appeared in response to the increasing availability of graphical Internet access and the accompanying pornographic web sites. The early versions of ICM software relied heavily on artificial intelligence (AI) to block access to pornographic or otherwise objectionable web sites. When a user attempted to access a web site that contained certain words or phrases, such as "XXX" or "sex", the screen would display a message informing the user that the filter was blocking access to the web site. Artificial intelligence is in fact quite good at identifying pornographic web sites, since pornographic web sites usually use a specific set of words such as "adult", "teen", "XXX", "porn", etc. to describe themselves. Some critiques of ICM software to this day leave the reader with the impression that ICM has never progressed beyond this early state.

It quickly became apparent that artificial intelligence software alone was not an acceptable solution to the challenges of Internet content management. AI technology has difficulty distinguishing between a news story about the Internet pornography business or an anti-pornography web site and a real pornography site. While some ICM vendors still offer products that rely on AI, the most widely used ICM products today either do not use AI or offer AI as a "fail safe" option the more cautious user may choose to enable.

Artificial intelligence is still heavily used as an intermediary step by the larger ICM vendors, including the one I work for, N2H2. Like other ICM vendors, N2H2 has found that sites identified by AI must then be subjected to human review to determine the content. Indeed, many Internet users are now discovering that automated search engines are a poor substitute for human review. [1]

Instead of relying on AI, N2H2 and our largest competitors rely on what is usually called "URL blocking" or "address blocking". URL blocking involves the compilation of lists of web site URLs (Uniform Resource Locator) that have been determined by a human reviewer to belong to a content category. Early versions of URL blocking software typically offered users a small numbers of the most obvious categories of sites users would find objectionable, such as "pornography", "hate speech", or "bomb making", or simply bundled all such objectionable material into a single category.

As the popularity of these URL blocking software programs spread, customers began to ask vendors to supply more categories and finer "granularity" in category selections. Schools didn't want students using web-based chat or e-mail. Corporations didn't want employees visiting sport sites or engaging in on-line trading. Libraries wanted to block pornography but not artistic nudity or sex education materials.

This market-driven push for greater flexibility and granularity led to the evolution from "filtering software" to Internet content management technologies. Today's ICM vendors offer customers an abundance of choices. N2H2 currently offers 34 categories with six "allow exceptions", allowing for hundreds of possible combinations. [2] WebSense offers 65 categories, [3] I-Gear 24 categories, [4] SmartFilter 31 categories, [5] X-Stop 28 categories, [6] Cyber Patrol 12 categories, [7] and SurfWatch 21 categories. [8]

A decision by an organization to purchase ICM software offers literally thousands of possible options, enabling diverse users such as Internet service providers, schools, business, libraries, government agencies, and individuals to choose a solution that meets very specific needs. By empowering choice, ICM technology liberates organizations from "one-size-fits-all" Internet access.

The widespread acceptance of ICM technology offers compelling testimony to the success of the ICM approach. According to a recent International Data Corporation survey, 82 percent of companies with more than 1,000 employees plan to purchase ICM software over the next 12 to 24 months. [9] A May 1999 report by Quality Education Data estimates that increased usage of ICM software in K-12 schools will increase to 71.5% in the 1999-2000 school year over the current 52.5% of U.S. school districts that used ICM in the 1998-1999 school year. [10] Hundreds of Internet service providers, including industry leader America Online, offer consumers the choice of filtered Internet service. The compatibility of ICM technology with good service was underscored recently when the Gwinnett County (GA) Library System, a public library that filters all Internet access, was given the prestigious "Library of the Year" award by Library Journal. [11]

Critics of ICM technology sometimes invoke the fear that individuals using ICM will somehow suffer because they will be denied access to vital information. Typical examples that are given of potential harms caused by ICM are students who will be placed at a competitive disadvantage because they will be unable to master the Internet, teens who will become pregnant or contract a venereal disease because they will be denied access to sexual health information, and gay teens who will suffer from depression or even commit suicide because they were denied access to gay web sites.

Such hyperbole has yet to be shown to match reality. Despite the fact that literally millions of students have relied on ICM enabled Internet access for years, ICM critics present no studies or statistics to suggest that these students are any less computer literate, well-educated, or emotionally well-adjusted than peers who use unfiltered Internet access. Further, ICM critics fail to even cite a single anecdote of any teen ever becoming depressed, contracting a venereal disease, becoming pregnant, committing suicide, or even receiving a bad grade on a paper because of ICM software.
Millions of Americans depend on Internet access using ICM technology as their primary means of accessing the Internet. Today's ICM technology is woven into the fabric of mainstream Internet access.

III) How Internet content management technology works.

As explained in the previous section, ICM technology involves the use of "block lists" of human-reviewed web sites which administrators can choose to enable or disable. Most vendors of ICM lists select the content of these lists based on carefully defined, objective, and openly published standards.

Probably the most objective and granular ICM lists involve material of a sexual nature. N2H2 has six categories devoted to sexual material, "Adults only", "Lingerie", "Nudity", "Porn", "Sex", and "Swimsuits". Additionally, N2H2 has four "Allow exception categories" related to sexual material: "Education", for sexually explicit material that is of an educational nature, "History", for material of historic value, such as the Starr Report, "Medical", for material such as photographs of breast reduction surgery, and "Text", for pornographic or sexual material that only contains text.

Websense offers five sex-related categories:

> *Adult content. Sites featuring full or partial nudity reflecting or establishing a sexually oriented context, but not sexual activity (3.3);sexual paraphernalia; erotica and other literature featuring, or discussions of, sexual matters falling short of pornographic; sex-oriented businesses such as clubs, nightclubs, escort services, password/verification sites Includes sites supporting online purchase of such goods and services.*
>
> *Nudity. Sites offering depictions of nude or seminude human forms, singly or in groups, not overtly sexual in intent or effect.*
>
> *Sex. Sites depicting or graphically describing sexual acts or activity, including exhibitionism.*
>
> *Sex Education. Sites offering information on sex and sexuality, with no pornographic intent.*
>
> *Lingerie and Swimsuit. Sites offering views of models in suggestive but not lewd costume; suggestive female breast nudity. Also classic "cheesecake" art and photography.* [12]

I-Gear offers seven sex-related categories:

> *Sex/Acts*
> *Sites depicting or implying sex acts, including pictures of masturbation not categorized under sexual education. Includes sites selling sexual or adult products.*
> *Sex/Attire*
> *Sites featuring pictures that include alluring or revealing attire, lingerie and swimsuit shopping areas, or supermodel photo collections but do not involve nudity.*
> *Sex/Personals*
> *Sites dedicated to personal ads, dating, escort services, or mail-order marriages.*
> *Sex/Nudity*
> *Sites with pictures of exposed breasts or genitalia that do not include or imply sex acts. Includes sites with nudity that is artistic in nature or intended to be artistic, including photograph galleries, paintings that may be displayed in museums, and other readily identifiable art forms. Includes nudist and naturist sites that contain pictures of nude individuals.*
> *Sex Education [Super Category] SexEd/Basic*
> *Sites providing information at the elementary level about puberty and reproduction. Includes clinical names for reproductive organs (e.g., penis).*

> *SexEd/Advanced*
> *Sites providing medical discussions of sexually transmitted diseases such as syphilis, gonorrhea, and HIV/AIDS. May include medical pictures of a graphic nature. Sites providing information of an educational nature on pregnancy and family planning, including abortion and adoption issues. Sites providing information on sexual assault, including support sites for victims of rape, child molestation, and sexual abuse. Sites providing information and instructions on the use of birth control devices. May include some explicit pictures or illustrations intended for instructional purposes only. May include slang names for reproductive organs, or clinical discussions of reproduction.*
> *SexEd/Sexuality*
> *Sites dealing with topics in human sexuality. Includes sexual technique, sexual orientation, cross-dressing, transvestites, transgenders, multiple-partner relationships, and other related issues.* [13]

N2H2 and other ICM vendors have developed a number of techniques for identifying web sites to add to our lists. The most common technique is the use of "robots": automated programs the search the web for web sites that contain certain words and phrases included in domain names, meta tags, or page text. N2H2 has 70 servers devoted to searching the web for candidate sites, along with multiple T3 and T1 lines to provide adequate bandwidth. This initial "catch" of candidate URLs is then matched against our existing database, and subjected to more complex AI algorithms. These automated processes continuously feed a list of sites to N2H2's review department.

ICM vendors also employ other methods to identify content to be rated. ICM vendors make use of content already indexed in the various search engines to identify candidate URLs using "search parasites." N2H2 makes use of a technique called "spidering", where a "robot" program retrieves URLs linked to pornography sites, particularly "pornography search engines" such as Persian Kitty and Naughty.com. Another technique N2H2 uses is performing "whois" searches of domain name registries for new domain name registrations that contain words commonly association with pornography sites such as "xxx" or "adult". Finally, N2H2 monitors Usenet newsgroups and e-mail lists devoted to announcing new pornography sites.

Further, nearly all of the sites ICM companies are trying to find are also trying to be found by users. Many sites, particularly commercial pornography sites, go to great lengths to be found by users, and thus are easily found by ICM companies. Even the more elusive sites, such as child pornography and illegal software pages, want to be found by their end users. This is one of the reasons that filtering the Internet is possible. Content placed on the Internet without anyway for anyone to find it really doesn't pose much of a threat to anyone.

The N2H2 review department consists of approximately 120 full-time and part-time reviewers. The N2H2 review department has a full-time equivalent (FTE) complement of 60 employees, employed 40 hours per week. N2H2 employs reviewers fluent in 15 languages, to keep up with the increasing internationalization of the Internet. These 60 FTE review staff spend 2400 person hours each week reviewing approximately 75,000 URLs, which are added to our database of millions of URLs that that N2H2 has reviewed since 1995. This translates into about two minutes spent reviewing each URL. About one in 4 URLs identified by AI as candidates for adding to our category lists are actually added. Therefore, each week about 20,000 new URLs are added to our category lists that are currently at 4.7 million URLs. Each URL effects 1 or many web pages. One method of calculating the number of webpages tagged for filtering shows over 15 million indexed webpages.

With the size of the World Wide Web estimated at 1.5 billion pages, [14] and new web sites appearing at a rate of 4,400 per day, [15] the task of keeping up with new web sites seems daunting. However, ICM vendors are not interested in reviewing *every new web page*, nor is their any need to do so. ICM vendors need only concern themselves with *new web sites featuring content that needs to be rated, or significant changes in the content of already-rated web sites*. The studies of the current size and growth of the web do not tell us what fraction of "new web pages" corresponds with "new web sites featuring content that needs to be rated, or significant changes in the content of already-rated web sites". While the Lawrence-Giles study found that 1.5% of web pages were pornographic, they did not find what portion of new web pages were new pornography sites. Therefore, it does not follow that statistics of the rate of web growth can be used to claim that keeping up with the growth of new web sites with content that needs to be rated is unlikely or impossible. Based on N2H2's internal sampling and customer feedback, N2H2 feels confident that we have adequate resources to keep up.

The criteria used to rate URLs are both public and well defined, but the actual lists of URLs are not made public by nearly all ICM vendors. There are two obvious reasons for this. First, as described earlier, a great deal of human labor is involved in creating these lists. Creating N2H2's list of 4 million+ reviewed URLs required hundreds of thousands of person hours, at a cost of quite literally, millions of dollars. Very few companies would willingly give away such expensive and valuable proprietary data. Second, it would be irresponsible to publish a gigantic list of pornographic web sites, as this information might well land in the hands of children. This point was illustrated graphically last month when Burger King restaurants in the United Kingdom gave away a CD-ROM to children that contained a filter with a published list of over 2,000 pornographic web sites. After complaints from parents and child safety groups, Burger King recalled the CD-ROM. [16]

If a user or webmaster is concerned that a particular site might be wrongly included on an ICM vendor's list, nearly every ICM vendor has e-mail links where such a request can be made. The makers of Cyber Patrol, SurfWatch, and WebSense provide on their web sites a search function where anyone can check to see if a URL is currently being blocked. [17] N2H2 takes this concept one step further by providing a link at the bottom of every web page in our ResourceBar, where an end user who encounters a site they feel is wrongly blocked can instantly send feedback to N2H2's review staff. The end user has the choice of submitting the request for review anonymously, or providing their e-mail address in order to get a response.

IV) Evidence of the effectiveness of ICM technologies

Research on the effectiveness of ICM technologies has been highly politicized. Nearly all of the research has been conducted by individuals with a strong bias for or against ICM (and I of course include myself here). Nearly all of the research, and I include some of my own work here, involves samples that are far too small. As my co-panelist Christopher Hunter rightly points out:

> *The majority of reports of Internet content filters being both underinclusive (failing to block the worst pornography, hate speech, violence, etc.), and overinclusive (blocking non-sexual, non-violent content), have come from journalists and anti-censorship groups who have used largely unscientific methods to arrive at the conclusion that filters are deeply flawed.* [18]

Studies using small samples

"Faulty Filters: How Content Filters Block Access to Kid-Friendly Information on the Internet", December 1997. Electronic Privacy Information Center. [19]
This study was conducted by the Internet free speech organization EPIC. EPIC states on its web site that "content filtering has been shown to pose its own significant threats to free expression on the Internet." [20] EPIC makes the striking claim that in EPIC's testing users were "denied access to 99 percent of material that would otherwise be available without the filters." However, EPIC did not actually test Internet filters to arrive at this figure, they tested an experimental filtered search engine using AltaVista in conjunction with the ICM product Net Shepherd. At the time of the study, AltaVista limited search results to 200 URLs, hence the "99%" blocked results. Further, EPIC did not use a fixed sample: researchers simply attempted to perform searches.

"The Internet Filtering Assessment Project", Karen Schneider, 1997. [21]
"The Internet Filtering Assessment Project" is the work of a critic of ICM software, Karen Schneider. Schneider used a team of 40 volunteers to test filters and found that "Over 35% of the time, the filters blocked some information they needed to answer a question." [22] Like the EPIC study, Schneider used a loose and open-ended searching method to determine if filters wrongly blocked sites. Schneider herself accurately described her work in her summary:

> *TIFAP was not a scientific study; it lacked controls, the actual conditions could not be verified, and, due to limited volunteers and resources, we could not consistently test all products the same way. The survey instruments are as amateurish as you would expect from people who do not design surveys.* [23]

Schneider tested mostly word-blocking filters by attempting to perform searches for information designed to trip word-blockers, such as "nursery rhymes, (pussycat, pussycat)". [24]

Censorware Project Reports
The Censorware Project, a group that describes its mission as "dedicated to exposing the phenomenon of *censorware*: software which is designed to prevent *another person* from sending or receiving information, usually on the web. A gag or blindfold is the physical equivalent of what such software does." [25] From 1998 to the present, the Censorware Project has issued a series of reports detailing URLs wrongly blocked by ICM vendors. With the exception of an analysis of Utah logs (see next section, "Studies using large samples"), the reports issued by the Censorware project do not attempt to set the

occurrence of "misblocks" in any context.

The Censorware Project lists four reports exposing misblocked web sites by ICM products. 26. Cyber Patrol is charged with 67 misblocks, 27 Websense with 12 misblocks, 28 X-Stop with 50 misblocks, 29 and Bess with 34 misblocks. 30

Unfortunately, no context for this information is provided, such as whether these small numbers of misblocks constitute all sites wrongly blocked by each filter or how big an impact these blocks would have on typical Internet traffic. Therefore, the only conclusions that can be drawn from this information is that these ICM products have been shown to block a small number of URLs incorrectly.

"Filtering the Future? Software, Filters, Porn, PICS and the Internet Content Conundrum" Christopher Hunter, 1999. 31
"Filtering the Future", a master's thesis by Christopher Hunter claimed that Internet filters "improperly block 21% of benign content". 32 The sample used in the study was a non-random sample of 200 sites. The study tested for blocking of "sex", "profanity", "nudity", and "violence", with ICM products configured to block all categories, including "gambling" and "alcohol", against a sample of "purposefully selected" sites, including gambling and alcohol sites, which were then counted as "wrongly blocked". Mr. Hunter later stated:

> *I readily admit that I need a better sample and that my results shouldn't necessarily be generalized to the entire universe of web pages.* 33

"A Guide to Filtering Software", David Burt, Parts I and II, 1999. 34
In 1999 I was asked to write two articles for "Dr. Laura Perspective Magazine" reviewing ICM products. My intention was not to conduct a scientific survey but to offer more of a "thumbnail sketch" of product reviews.
I reviewed 14 ICM client products and "clean ISPs". For this review I selected 250 web sites, 100 randomly selected pornography sites, 75 purposefully selected sites promoting drugs, hate, and bomb-making, and 75 purposefully selected "innocent sites" related to gay rights, feminism, breast cancer, and news stories about hate speech and online pornography. The various products were between 85% and 99% effective at blocking pornography, and less effective at blocking other undesirable sites. Most of the products blocked none of the "innocent sites", while several, particularly the AI-based products did block innocent sites.

Studies using large samples

Considering the vast size of the Internet, and the fact that ICM products are only targeting a small portion of the Internet, it quickly becomes obvious that the only way to accurately test ICM products is to test against large samples of URLs. Fortunately, two such tests have been conducted, "Censored Internet Access in Utah Public Schools", a study of SmartFilter by Michael Sims of the Censorware Project, and "Dangerous Access, 2000 Edition", a study of Bess and Cyber Patrol, by David Burt. Even though Mr. Sims and myself are on opposite sides of the debate over the effectiveness of ICM software, the bottom-line findings we both arrived at over ICM error rates were remarkably similar.

"Censored Access in Utah Public Schools", by Michael Sims, 1999. [35]
In 1998, anti-filtering activist Michael Sims obtained one month's worth of Internet log files from the Utah Education Network, which provides Internet access for nearly all of Utah's public schools. The Utah schools use an ICM product, Smart Filter. In March of 1999, Sims issued a report analyzing the filtered log files. The logs recorded 53,103,387 total files accessed, of which 205,737 were blocked, 193,272 under the Smart Filter "sex" category. When Sims removed banner ads and image files, achieving a rough approximation of "page views", Sims records the numbers as 15,434,442 pages accessed, of which 95,059 were blocked, 86,957 under the Smart Filter "sex" category. Sims reported about 300 pages wrongly blocked. On June 28, 1999 the Censorware Project wrote a follow-up report that listed the total number of wrongly blocked pages at 5,601, but did not list all the actual pages. [36] The 5,601 wrongly blocked pages Sims found out of 15,434,442 pages accessed results in an error rate of .036%.

"Dangerous Access, 2000 Edition", by David Burt, 2000. [37]
As part of a report discussing the spread of Internet pornography I analyzed the filtered log files of two public libraries earlier this year. I found that Cyber Patrol used at the Tacoma (WA) Public Library wrongly blocked 1,853 pages out of 2,510,460 pages accessed, or .073%, and that Bess used at the Public Library of Cincinnati and Hamilton County wrongly blocked 732 pages out of 3,717,383 pages accessed, or .019%.

The advantages of log analysis studies versus studies involving small, purposefully selected samples are both considerable and obvious. First, a researcher with a possible bias is not creating the sample of URLs used, they are being taken directly from a real-world sample. Second, the size of these samples makes it much more likely that they will accurately reflect real-world conditions. Third, the rate of overall blocking by the ICM product is not being determined by the researcher, but rather is part of the original sample.

Even with these advantages, a researcher evaluating log files must still make decisions about which blocks have been applied incorrectly. Mr. Sims and myself used somewhat different criteria for evaluating "wrongly blocked" web sites. I included most sexually explicit material as being correctly within the parameters of the filtering categories used by Cyber Patrol and Bess. Mr. Sims, on the other hand, counted as wrongly blocked many sexually-themed web sites such as www.playboy.com, commenting that "Besides the photographs, Playboy of course has many interviews and well-written articles." [38]

In spite of these differences in attitude, it is well worth noting that both log analyses came to very similar conclusions about the level of inappropriate blocking. Sims found that Smart Filter wrongly blocked .036% of the time, and I found that Cyber Patrol wrongly blocked .073% of the time, and that Bess wrongly blocked .019% of the time. This suggests that the expected error rate for the most commonly used ICM products is a few hundredths of one percent, and it is my belief that further study will verify this.

V) Suggestion for further study

My own interpretation of what the evidence gathered to date suggests is that the best ICM products accurately block over 90% of pornographic web sites, and erroneously block less than .1% of non-pornographic web sites.

However, in order to come to more solid conclusions about the effectiveness of ICM software, a rigorously scientific testing of ICM products against a large sampling of both pornographic and non-pornographic URLs should be conducted. I first proposed such testing in December of 1998, when I testified before the National Commission on Library and Information Science:

> *Because of this lack of reliable data, I'd like to suggest that this commission take the lead in producing better data. I think that conducting a study that could tell us what we need to know would be pretty straightforward. Such a study would involve writing a special computer program that would run on Internet workstations in several public libraries that either filter for all patrons, or just for all minor patrons. First, the program would record the address of every website that every patron visited. Second, the program would record the address of every website someone tried to access, but was blocked by the filter. Third, the program would record if the filter were overridden in any of the cases where a patron encountered an inappropriate block. With this method we could actually get a reasonable idea of: 1) What exactly are patrons being prevented from viewing in libraries that filter, 2) How often are patrons prevented from viewing web sites they want to access, and 3) When a patron encounters an inappropriately blocked website, how likely are they to ask to see it.* [39]

Unfortunately, NCLIS did not express any interest in facilitating such a study. I find it heartening now to hear others, such as my co-panelist Mr. Hunter, also expressing the need for more rigorous studies on ICM effectiveness. Since I testified before NCLIS, my thoughts on how to conduct an ICM study have evolved.

The purpose of such a study should be twofold: 1) to determine how effective filters are at blocking pornographic web sites; 2) to determine the extent of "overblocking" of innocent web sites on Internet access. To this end two sets of data would be needed: a large sampling of pornographic web sites, and a large sampling of "typical" web traffic.

I would propose that the study be conducted by a reputable research facility well versed in software testing methodologies, using standard laboratory control procedures. The ICM vendors themselves could fund the study.

There are a number of ways to obtain the required data. The participating vendors themselves could each supply several thousand pornographic URLs to form a combined list that would be tested against all products. Alternatively, the pornographic URLs could be obtained through search engines and pornographic directory sites such as Naughty.com. The larger the sample the better, and I think a minimum of 25,000 unique pornographic URLs would be required.

The "typical" Internet traffic could be obtained from the log files of a university, library, or Internet Service Provider, then reduced to only unique web page files. I think a minimum of 250,000 unique pages would be required.

BEST COPY AVAILABLE

A lab could set up a server for each ICM product, with each product configured to block only pornography, then simultaneously run scripts containing the test data against each product. Once the testing was complete the results could be measured to determine 1) the percentage of pornographic URLs blocked by each product; 2) the percentage of typical web traffic blocked by each product.

More difficult is determining the amount of "wrongly blocked" URLs. Each URL from the "typical" web traffic data that was blocked would have to be examined and judged to be "rightly blocked" or "wrongly blocked". Considering that 1% to 3% of the "typical" web traffic would likely be blocked, this would involve thousands of URLs. N2H2's experience has been that it requires on average 2 minutes to review a URL. If the testing generated 10,000 blocked URLs, this would require 333 person hours to examine. Additionally, there would likely be some difference among the reviewers as to what was wrongly blocked, so ideally two different reviewers should review each URL.

In a debate over ICM software that has been full of heated rhetoric and weak research, solid, objective data is sorely needed. I would ask this commission to please consider making such a study possible.

Thank You.

Footnotes

1. Lisa Guernsey, "The Search Engine as Cyborg", *The New York Times*, June 29, 2000.
2. N2H2, *Human Review Filtering Solution*, http://www.n2h2.com/solutions/filtering.html.
3. WebSense, *Websense 4: Database Categorization Criteria*, http://www.websense.com/products/categories/version4.cfm
4. URLabs, *URLabs content category definitions*, http://www.symantec.com/urlabs/public/support/faq/categories.html
5. Secure Computing, *Frequently Asked Questions*, http://www.securecomputing.com/index.cfm?sKey=275
6. X-Stop, *X-Stop XLM for Microsoft NT Proxy Manual*, http://www.xstop.com/docs/Manual_xlm_msnt30b.pdf
7. Cyber Patrol, *Category Definitions - 1/20/99*, http://www.cyberpatrol.com/cybernot/criteria.htm
8. SurfWatch, *How we filter*, http://www1.surfwatch.com/about/filter.html
9. Chris Christiansen, "Worldwide Market for Corporate Internet Access Control", *International Data Corporation*, July 1999.
10. Quality Education Data, *Internet Usage in Public Schools, 4th edition*, 1999.
11. Library Journal, *Library of the Year*, June 15, 2000.
12. WebSense, *WebSense 4: Database Categorization Criteria*, http://www.websense.com/products/categories/version4.cfm
13. URLabs, *URLabs content category definitions*, http://www.symantec.com/urlabs/public/support/faq/categories.html
14. David Lake, "The Web: Growing by 2 Million Pages a Day", *The Industry Standard*, February 28, 2000, http://www.thestandard.com/research/metrics/display/0,2799,12329,00.html
15. Lake.
16. Jonathan Lambeth, "Burger King gives away porn addresses", *UK Telegraph*, June 26, 2000.
17. SurfWatch "Test-a-Site", http://www1.surfwatch.com/testasite/. Cyber Patrol "CyberNot Search Engine", http://www.cyberpatrol.com/cybernot/. WebSense, "Site Look Up", http://database.netpart.com/site_lookup.html.
18. Christopher Hunter, *Cyberporn, Filters, and Public Policy: A Content Analysis Research Proposal study proposal*, 2000.
19. EPIC, *Faulty Filters: How Content Filters Block Access to Kid-Friendly Information on the Internet*, December 1997. http://www.epic.org/Reports/filter_report.html.
20. EPIC, *Filters and Freedom*, http://www.epic.org/bookstore/filters&/.
21. Karen Schneider, *The Internet Filtering Assessment Project*, 1997, http://www.bluehighways.com/tifap/learn.html.
22. Schneider.
23. Schneider.
24. Schneider.
25. Censorware Project, *Welcome to Censorware.org*, http://www.censorware.org/intro/
26. Censorware Project, *Censorware Project Special Reports*, http://www.censorware.org/reports/

27. Censorware Project, *Blacklisted by Cyber Patrol: From Ada to Yoyo*, December, 1997, http://www.censorware.org/reports/cyberpatrol/ada-yoyo.html.
28. Censorware Project, *Protecting Judges Against Liza Minnelli: The WebSENSE Censorware at Work*, June, 1998, http://www.censorware.org/reports/liza.html
29. Censorware Project, *The X-Stop Files: Deja Voodoo*, http://www.censorware.org/reports/xstop/. The Censorware Project may have found other misblocks as well. Just before the X-Stop report was released the ACLU issued a "statement of undisputed facts" that stated there were "Well Over a Hundred Sites Have So Far Been Identified by Library Staff, Patrons, Intervenors, and Others That Were Blocked Even Though They Did Not Violate The Policy and Contained Constitutionally Protected Speech". See http://www.aclu.org/court/loudoun_facts.html.
30. Censorware Project, *Passing Porn, Banning the Bible: N2H2's Bess in public schools*, http://www.censorware.org/reports/bess/
31. Christopher Hunter, *Filtering the Future? Software, Filters, Porn, PICS and the Internet Content Conundrum*, 1999.
32. Hunter.
33. David Burt, *ALA touts filter study whose own author calls flawed*, 2-18-2000, http://www.filteringfacts.org/hunter.htm.
34. David Burt, "A Guide to Filtering Software", *Dr. Laura Perspective*, July, 1999, p. 12; And David Burt, "An Update on Filtering Software", *Dr. Laura Perspective*, October, 1999, p. 14.
35. Michael Sims, "Censored Access in Utah Public Schools", *Censorware.org*, March 1999, http://www.censorware.org/reports/utah/main.shtml.
36. Jamie McCarthy, "Lies, Damn Lies, and Statistics: A followup to our March 1999 Utah SmartFilter report", June 28, 1999, http://www.censorware.org/reports/utah/followup/.
37. David Burt, *Dangerous Access 2000 Edition*, March 1999.
38. Sims. http://www.censorware.org/reports/utah/appendix.shtml.
39. David Burt, *Testimony before the National Commission on Library and Information Science*, November 10, 1998, http://www.filteringfacts.org/nclis.htm.

Supplemental Testimony of David Burt
September 1, 2000

Thank you the opportunity to address the COPA Commission on the topic of the effectiveness of Internet Content Management software. It was a pleasure to be able to discuss some of the evidence gathered to date about the effectiveness of filtering software.

As I stated in both my written and oral testimony, it is well worth noting that all log analyses studies of large amounts of filtered Internet traffic have come to very similar conclusions about the level of inappropriate blocking. The number of "wrongly blocked" pages Michael Sims of the Censorware Project found divided by the total number of pages accessed for Smart Filter results in an error rate of .036%. I found that Cyber Patrol wrongly blocked .073% of the time, and that Bess wrongly blocked .019% of the time. This suggests that the expected error rate for the most commonly used ICM products is a few hundredths of one percent.

My co-panelists, Karen Schneider and Christopher Hunter, did not dispute this claim. Rather, Mr. Hunter stated that "even a filter that was 99.999% accurate" would still not be "Constitutional", though Mr. Hunter cautioned that he was not an attorney. Hunter's sentiments echoed those of Karen Schneider, who in earlier testimony to the National Commission on Library and Information Science stated:

> *In attempting to demonstrate that filters only limit negligible amounts of free speech – as if there were such a standard – he* [Mr. Burt] *has unwittingly underscored my argument. Imagine if NCLIS heard that private organizations were slipping into libraries at night and removing books, and that Mr. Burt then testified that there were only a negligible amount removed, after all, (to use his term) "by mistake." Surely the NCLIS would agree that there is no tolerable level for the censorship of protected speech.* [1]

In this passage Ms. Schneider compares filtering to the removal of books. I have argued that the matter is more complex than this simple analogy. In my Expert Report filed in *Mainstream Loudoun*, I quoted form COPA Commission NAS Panelist Marilyn Gell Mason:

> *Filtering cannot be rightly compared to "selection", since it involves an active, rather than passive exclusion of certain types of content. But filtering cannot be rightly called "removal" either, since the materials being "removed" do not exist in the library and were never consciously selected by the librarian. Filtering is best described as being somewhere between selection and removal. Marilyn Gell Mason, the director of the Cleveland (Ohio) Public Library, recently said "When we make judgments we call it selection. When we choose to exclude material we call it censorship. Evidence suggests that the distinction lacks meaning in an electronic environment." (Mason, 1997)*[2]

It should be noted that in other instances, such as her report on filtering software written for GLAAD, Ms. Schneider also appears aware of these complexities, stating that:

> *Filtering is extremely similar to the failure to select books* [3]

In her testimony, Ms. Schneider is generally dismissive of documented incidents of patrons accessing pornography in libraries, characterizing these as

> *isolated incidents involving situations where one person saw another person viewing something that the first person felt was inappropriate or objectionable.* 4

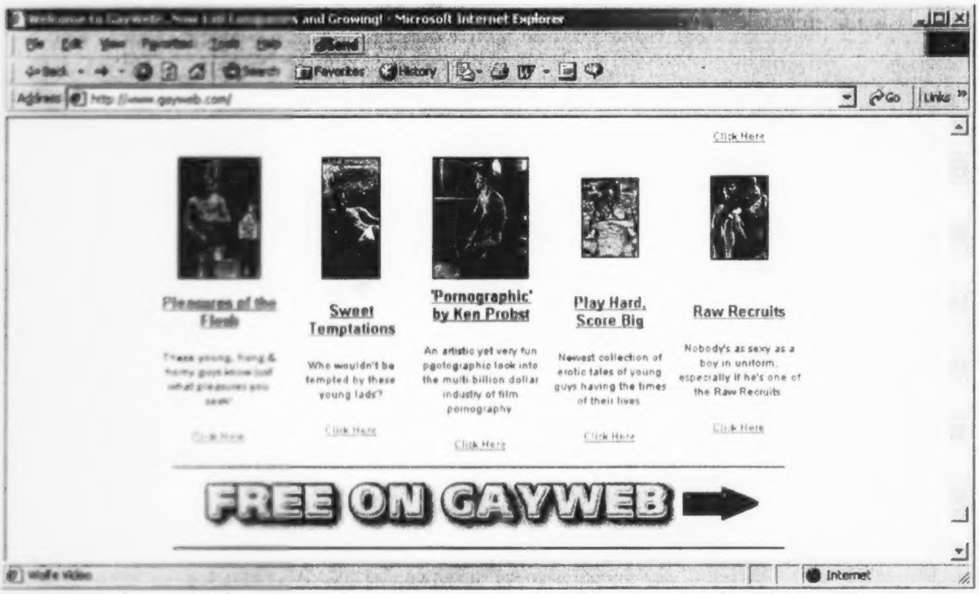
Yet as Ms. Schneider herself has repeatedly stated, complaints about Internet filtering problems are the "tip of the iceberg":

> *As I stated on Web4Lib, there have been *no* end-user studies of filters in libraries, and we do not measure library services by the number of complaints we receive. Complaints (while not to be ignored) are "tip of the iceberg" information.* 5

Ms. Schneider repeatedly mentions a "gay-themed jewelry site" in her testimony:

> *I argued that a gay-themed jewelry site should not be blocked; Mr. Burt argued that is should be blocked because its hosting site was "porn" (though he did not explain why the jewelry site fit into this category)* 6

However, Ms. Schneider does not provide the reader with the name or the URL of either the "parent site", or the "jewelry site", so that readers may decide for themselves whether or not filtering is appropriate. The site is called "Gay Web", and is available at http://www.gayweb.com. This site is blocked under sex-related categories by Cyber Patrol, SurfWatch, Bess, I-Gear, X-Stop, Net Nanny, Cyber Sitter, and WebSense. In short, *it is blocked by every major filter*. The content of the site, whose index.html page alone features dozens of photographs of nude men and much sexually explicit language, speaks for itself:



Pleasures of the Flesh

These young, hung & horny guys know just what pleasures you seek!

Click Here

Sweet Temptations

Who wouldn't be tempted by these young lads?

Click Here

'Pornographic' by Ken Probst

An artistic yet very fun pgotographic look into the multi billion dollar industry of film pornography

Click Here

Play Hard, Score Big

Newest collection of erotic tales of young guys having the times of their lives

Click Here

Raw Recruits

Nobody's as sexy as a boy in uniform, especially if he's one of the Raw Recruits

Click Here

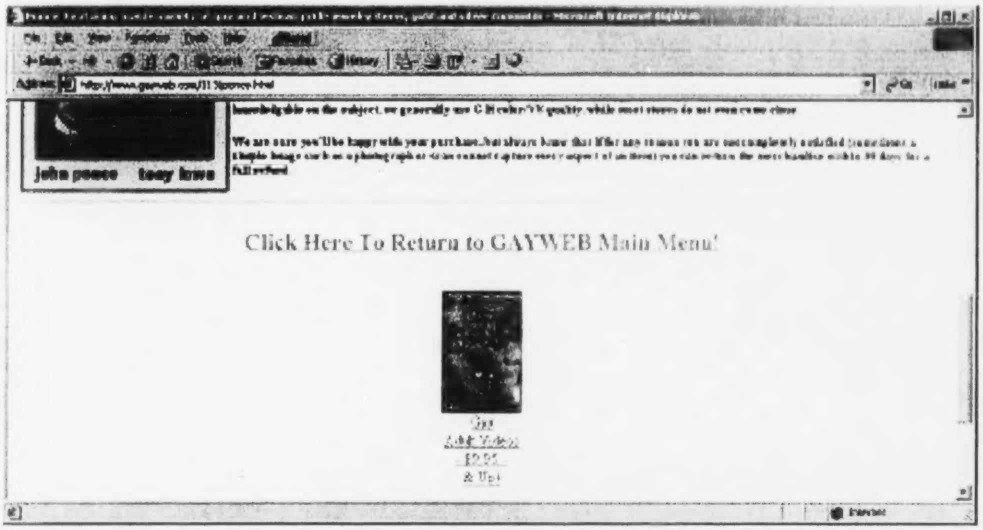
The text shown in the above screen capture reads, "Pleasures of the Flesh --These young, hung & horny guys know just what pleasures you seek! Click Here", "Sweet Temptations -- Who wouldn't be tempted by these young lads? Click Here", "Pornographic by Ken Probst --An artistic yet very fun photographic look into the multi-billion dollar industry of film pornography. Click Here", "Play Hard, Score Big -- Newest collection of erotic tales of young guys having the times of their lives. Click Here","Raw Recruits--Nobody's as sexy as a boy in uniform, especially if he's one of the Raw Recruits. Click Here."

BEST COPY AVAILABLE

Ms. Schneider objects to classifying any of the material on Gay Web as "porn". However, Ms. Schneider does not explain how she is able to define what pornography *is not*, since when giving sworn testimony as an expert on software designed to block pornography, she could not define what pornography *is*. From Ms. Schneider's sworn deposition in *Mainstream Loudoun*:

> *Q. [Defendant's attorney Ken Bass] What is pornography?*
> *A. [Witness Schneider] Study of porn.*
> *Q. Do you seriously as a person with a master of science think that pornography is the study of porn?*
> *A. Look, I don't know what pornography is...*
> *Q. And as you sit here today, you're telling me under oath that you have no understanding as a person of the term pornography?*
> *A. No.* 7

Content similar to that found on http://www.gayweb.com/index.html is featured throughout the Gayweb site, including the "jewelry site". This consists of pages of Gayweb related to jewelry, and is located at http://www.gayweb.com/113/ponce.html. Again, this subpage is blocked by every major filter. Again, the content, advertising "Gay Adult Videos" and showing nude men, speaks for itself:



Unfortunately, Ms. Schneider appears to regularly engage in the tactic of fabricating baseless charges of homophobia against those who support the use of filters. In Ms. Schneider's GLAAD report she made such a charge against the organization "Enough is Enough", labeling EIE "actively homophobic", and accusing EIE of being "involved in reducing gay rights":

> *We know a lot about the organizations that encourage mandatory filtering; filtering proponents are nearly all from the far right, including the Family Research Council, Enough is Enough, Family Friendly Libraries, and the American Family Association. All of these organizations have extensive credentials in other censorship areas; restriction, removal and prevention of information flow are crucial to their mission. Not coincidentally, all of these groups are actively homophobic, and not only promote anti-gay rhetoric but have been involved in reducing gay rights...* **8**

BEST COPY AVAILABLE

This characterization of the group Enough is Enough not only without foundation, it is actually *refuted* by an item on GLAAD's own web site:

> *In last week's GLAADAlert ("The Quest for Fairness on the 'Net"), the Web site of the anti-pornography group Enough is Enough was criticized for its inclusion of a "victim testimonial" from a man who described himself as "ex-gay." After receiving numerous e-mails from GLAADAlert readers, Shyla Welch, director of communications for Enough is Enough, contacted GLAAD to discuss the issues raised in the Alert item. After a constructive dialogue, Welch and Enough is Enough agreed to remove the testimonial from their Web site.* [9]

Ms. Schneider also makes a number of misleading, and in some instances factually untrue claims about a report I wrote, "Dangerous Access 2000". These claims go beyond misrepresentations or distortions, and include fabricated statements and invented statistics which are not contained in "Dangerous Access 2000".

On page 14 of her testimony, Schneider characterizes my analysis of log files as:

> *Burt, whose assessment of what he construes to be "porn" is by his own admission very broad, still only found that between one-half and one-third of one percent of all Internet access was blocked by Internet filters, yet he justifies his concerns by claiming that each blocked site translates, in his words, into "thousands of separate incidents.* [10]

The statement "between one-half and one-third of one percent of all Internet access was blocked" is not found on the page Schneider cites, page 44, nor is it found *anywhere* in *Dangerous Access 2000.* The only place where the five log files mentioned in Dangerous Access 2000 are discussed in an aggregate way is on page 23, where a table shows *between 5.00% and .36%*, not "one-half and one-third of one percent, as Ms. Schneider dishonestly claims.

Further, Ms. Schneider fabricates a statement accredited to me, representing me as "claiming that each blocked site translates, into 'thousands of separate incidents". The sentence Ms. Schneider is partially quoting from does not discuss aggregate log files, as she implies, but discusses the logs of one library, the Cincinnati Public Library. The exact quote is:

> *While 0.53 percent of all web accesses may not sound significant, this translates into thousands of separate incidents in only a two month period, many of which very likely involved the illegal transmission of obscenity.* [11]

Nowhere is the claim here made, nor can it be extrapolated, that I am claiming that "each blocked site translates" into "thousands of separate incidents." What are counted as incidents in the Cincinnati data are not "each blocked site", but an entirely different statistic, "unique blocked clients", which has to do with the number of blocked user sessions, not websites. The precise meaning of the statistic "unique blocked clients" is defined on page 41:

> *Unique Blocked Clients represents the number of individual workstations from which Internet requests were blocked. A minimum number of unique user sessions where there were attempts to access blocked files can be drawn from this session.* [12]

Schneider continues this misrepresentation on page 15:

> *Burt, for example, claims that at one library there were over 4,000 "separate incidents," but he means that there were by his estimate 4,279 blocked sites that he "assumes" were sexually-explicit to the point where he, Burt, would expect them to be blocked, and which realistically were probably accessed in far fewer than 4,000 secessions.* [13]

The statistic "4,279 blocked sites" does not exist anywhere in *Dangerous Access 2000*. The Cincinnati log data, which Schneider is again referring to, on page 42 states there were "approximately 19,837 actual web pages were blocked", not the fabricated statistic of "4,279 blocked sites" Ms. Schneider presents. Again, the "over 4,000 separate incidents" is a measure of unique user sessions, not websites.

Schneider continues presenting fabricated statistics on page 15:

> *Furthermore, this library reported over 14 million websites accessed during this same period. 4,000 websites may seem like an enormous number – but within the context of total public use, dwindles to a pittance.* **14**

In this passage not only does Schneider continue to use the invented statistic of "4,000 websites", but introduces another fabrication, "14 million websites". The number of "websites" accessed in the Cincinnati logs is not defined in *Dangerous Access 2000*. Rather, the number of HTML pages is defined, on page 42, and it is 3,717,383, not 14 million. There is a figure given of 14,376,211 "total requests", but it is made clear on page 41 that this does not represent "web sites" or "web pages":

> *Total Requests represents the total number of all web-related files, such as html pages, as well as gif and jpg image files requested by Internet users.* **15**

On page 10, Ms. Schneider aggregates several statistics out of context to make another misleading claim:

A study by Burt showed that 15% of one filter's blocks were sites that were "non-sexual", "undeterminable", or "dead links", and to Burt, this was an effective filter." **16**

These statistics are not found not found on page 40 of *Dangerous Access 2000*, as Ms. Schneider claims. Rather, they are described in detail on pages 42-43:

> *Commercial Pornography Sites 76%*
> *Sexual Sites 9%*
> *Dead Links 6%*
> *Undeterminable 7%*
> *Nonsexual sites 2%*
> *Undeterminable URLs were portions of sites that served images or banners to meta-sites, and the directory or sub-page where the image was serving was not determinable.*
> *Dead Links were sites or relevant portions of sites that returned a "not found or "error message". Nonsexual sites were sites that had not sexual content at all.* **17**

This suggests a 2% error rate, not 15%. The 7% "undeterminable" sites are due to the fact that the log analysis *is based on sampling*, as is clearly described in the report. The high number of "dead links" is due to the fact that the logs are from July 1999 to September 1999, and were not analyzed until February 2000, and were therefore six months old when analyzed.

In closing, I would like to repeat my request for better filtering data. In order to come to more solid conclusions about the effectiveness of ICM software, a rigorously scientific testing of ICM products against a large sampling of both pornographic and non-pornographic URLs should be conducted. In a debate over ICM software that has been full of heated rhetoric and weak research, solid, objective data is sorely needed. I would ask this commission to please consider making such a study possible.

Thank You.

BEST COPY AVAILABLE

Footnotes

1. Schneider, Karen. (December 10, 1998). Written Material from the Garfield Library of Brunswick. Submitted by Karen G. Schneider, Director. In: *Kids and the Internet: The Promise and the Perils*, page 230.
   This position that even the smallest error rates are unacceptable is also echoed by the American Civil Liberties Union, which in their "Statement of Undisputed Facts" in the Mainstream Loudoun case held that "Well over a hundred sites have so far been identified by library staff, patrons, intervenors, and others that were blocked even though they did not violate the policy and contained Constitutionally protected speech", and this made filtering in a library unacceptable. ACLU. (1998). Plaintiff-Intervenors' Statement of Undisputed Facts", Available at http://www.aclu.org/court/loudoun_reply.html.
   Representatives of a group called "Mainstream Loudoun" in their own testimony submitted to the NCLIS report would characterize my statement that "[i]n the Loudoun County case, the plaintiffs claim that about 100 sites were inappropriately blocked by the filter X-stop." As "inaccurately describ[ing] the factual record", (*Kids and the Internet*, page 169.) despite the fact that the attorneys (the ACLU) *from Mainstream Loudoun's own side of the litigation* described the number of blocked sites as "well over a hundred." To add to the irony, in "refuting" my statement, Mainstream Loudoun was not even able to provide the names of 50 "wrongly blocked sites", much less "well over a hundred." (*Kids and the Internet,* pages 168-171)
2. Burt, David. (July, 1998). *David Burt Expert Report*, page. Available at http://www.filteringfacts.org/expert.htm.
3. Schneider, Karen. (2000). Access: The impact on the Lesbian, Gay, Bisexual and Transgender Community, page 12. In *Access Denied 2.0*, GLAAD.
4. Schneider, Karen. (July, 2000). *Testimony of Karen G. Schneider before the COPA Commission*, page 14.
5. E-mail message from Karen Schneider. (January 27, 1998). "Re: New Filtering Survey", in Publib. Available at http://sunsite.berkeley.edu/PubLib/archive/9801/0237.html
6. Schneider, Karen. (July, 2000). *Testimony of Karen G. Schneider before the COPA Commission*, page 11.
7. Deposition of Karen Schneider, Mainstream Loudoun, et al vs Board of Trustees of the Loudoun County Library, July 24, 1998. Page 140-41.
8. Schneider, Karen. (2000). Access: The impact on the Lesbian, Gay, Bisexual and Transgender Community, page 12. In *Access Denied 2.0*, GLAAD. Page 13-14.
9. GLAAD. (August 29, 1997). GLAADALERT FOLLOW-UP--ENOUGH IS ENOUGH SAYS "ENOUGH". Available at http://www.glaad.org/org/publications/alerts/index.html?record=1542.
10. Schneider, Karen. (July, 2000). *Testimony of Karen G. Schneider before the COPA Commission*, page 14.
11. Schneider, Karen. (July, 2000). *Testimony of Karen G. Schneider before the COPA Commission*, page 14.
12. Burt, David (March, 2000). *Dangerous Access 2000 ed.* Page 41.
13. Schneider, Karen. (July, 2000). *Testimony of Karen G. Schneider before the COPA Commission*, page 15
14. Schneider, Karen. (July, 2000). *Testimony of Karen G. Schneider before the COPA Commission*, page 15.
15. Burt, David (March, 2000). *Dangerous Access 2000 ed.* Page 41.
16. Schneider, Karen. (July, 2000). *Testimony of Karen G. Schneider before the COPA Commission*, page 10.
17. Burt, David (March, 2000). *Dangerous Access 2000 ed.* Page 42-43

Andrew N. Edmond

A Los Angeles native, Andrew N. Edmond is the Founder and CEO of SexTracker. At 27, he has risen to the top of the highly competitive online adult industry, establishing himself as one of the brightest young entrepreneurs on the Internet. In a short two years, he has taken SexTracker from a start-up business with two employees in the basement of his house, to a multi-million dollar company with over 100 employees.

In 1994, Edmond moved from Los Angeles to attend the University of Wyoming. In 1996, Edmond graduated with a B.S. in Botany and moved to Seattle, working at Real Networks for one year but knowing his destiny lay elsewhere. In 1997, he took his modest savings account and began building a site around what he believed was a completely untapped market in the online adult industry. Six months later, Edmond and Real Networks co-worker Ross D. Perkins had built several statistical programs specifically designed for the adult Webmaster. Since then SexTracker has become one of the most successful and profitable adult Web companies in the world.

Edmond is representative of a new generation of successful interactive media entrepreneurs. While he literally grew up with the Internet and has made exceptional use of its potential, he contends that the medium today is still in a primitive state. Edmond believes that in the next few years, as the

-more-

Internet blends with television it will become more convenient and more interactive, and he has laid the groundwork for SexTracker to become a technology rich resource for adult and mainstream Webmasters and surfers alike.

Says Edmond:

Flying Crocodile believes that the adult segment of online commerce is a fundamental component to many successful online e-commerce endeavors. No other market has shown and proven its willingness to deliver to consumers, using envelope pushing technical and marketing solutions to provide the content and products they seek in a cost effective manner. I believe the Adult Internet will form a strong symbiosis with non-adult marketing firms, technical solution providers, internet service providers, media companies and many other non-adult segments to deliver to consumers the desired product or service in the most cost effective, technically brilliant, and industry leading manner. As many other non-adult companies write themselves out of the marketplace in waves of red ink, the Adult Internet will continue to thrive, profitably, as it seeks to please the consumer using the latest and greatest sales techniques a

Testimonial of Andrew Edmond to the COPA Commission on the issues of Labeling, Rating, and Filtering

To the ladies and gentlemen of the COPA Commission, Congressional and Political Leaders, and the American Public:

My name is Andrew Edmond, CEO and President of Flying Crocodile Incorporated™.

Flying Crocodile's services are geared towards Adult webmasters and consenting Adult consumers, offering hosting, statistics and traffic analysis, customer service, advertising, leadership, industry news, and a host of additional subscriber services. Our current position in the Adult Online Industry is one of leadership, hosting over 80% of all free sites on the Adult web. This also places us in a position of responsibility that we have, not only to webmasters and Adult consumers, but to all of our visitors and the American public.

One of the product solutions that we have implemented to combat Online Child Pornography is iQcheck™, short for Internet Quality Check, which is internet software that tracks, reports to the FBI, and shuts down child pornography sites in our hub of over 120,000 adult websites. An iQcheck seal is displayed on participating web sites and links to an automated system which tracks all reports Flying Crocodile receives from the web-browsing public of abuse issues, such as copyright infringement, unsolicited bulk email (spam) and exploitation of minors. A visitor to an adult site who questions the content of a site, or who believes they have been spammed by a site that carries the iQcheck seal, can simply click on the seal itself to go directly to Flying Crocodile's iQcheck home page, where they may report the perceived abuse. The user will then be notified of any action taken as a result of their complaint and can revisit the iQcheck home page to track the status of their reports.

In terms of labeling, rating, and filtering solutions, I would like to address some of the solutions that have been presented.

While the proposition of XXX Domain is well intended, a XXX Domain, however, is not a global solution for the World Wide Web. It poses ethical risks to a diverse American public, financial burdens on Adult consumers and the Adult Online Community, as well as the assurance of biased censorship on the part of search portals.

There has been an influx in development of Filtering Services as with NetNanny, CYBERsitter, Cyber Patrol, Intel's Processor Serial Number (PSN), Jayde.com and an abundance of filters on the World Wide Web and solutions that range from filtering from the processor level, software level, to the ISP provider level.

The evident problems of filtering deal directly with the First Amendment and constitutionality of filtering in our diverse American society of ethnic, social, religious, and therefore, ethical diffusion of influences over our culture. A standard filtering system imposed by government or an oligarchy of corporate systems is inevitably unconstitutional.

The proposals of the Adult Online Community are as follows:

An evaluation, further consideration, and proposal of an Adult Online Community standard based upon labeling and rating systems proposed by the Internet Content Rating Association (ICRA), whom Flying Crocodile currently works with.

A community evaluation of Flying Crocodile's current service, iQcheck, and implementation across the scope of the Adult Web.

International consideration of applying these tools to the global World Wide Web and community evaluation of standards that we can impose to police the Adult Online Global Community.

In addition, services, such as BayTSP, exist to comply with existing law by aiding in verification of legal images.

These are self regulatory tools that Flying Crocodile proposes as strong solutions to continue and further our efforts in combating child access to the Adult Web and illegal images of children on the Adult Web and otherwise.

We are available, knowledgeable, and prepared to perform thorough investigations, research, and reports, use our coalitions in place and enhance the communication in the Adult Online Community to form a self regulating body on the web that adheres to the standards of the Commission and the American public to produce and apply innovative technical solutions to further combat these problems.

Thank you for the opportunity to present our ideas on this issue of mutual concern to Flying Crocodile, the Adult Online Community, the Commission, and the American public and be assured of our continued effort to address these concerns.

Bio - Scott Fehrenbacher

Scott joined Crosswalk.com, the nation's largest Christian Internet community, in 1998 when they acquired his company, the Institute for American Values Investing. Today Scott is Vice President of Crosswalk.com and is responsible for the content programming and development of ten channels at Crosswalk.com including the News & Culture, Spiritual Life, Money, Values-based Investing, Home Schooling, and other channels.

Before joining Crosswalk.com, Scott founded the Institute for American Values Investing; a national leader in providing cultural investment screening research to Wall Street. Based in Seattle, Washington, the Institute was the first organization to analyze and rate individual companies and mutual fund portfolios based on socially conservative screening criteria. The new methodology has been reviewed in many publications *including The New York Times, Boston Globe, Philadelphia Inquirer, London Sunday Telegraph, Dallas Morning News, International Herald Tribune*, as well as *Money, Business Week, Mutual Fund, New Republic, Institutional Investor,* and *American Banker* magazines. Scott has also appeared on CNBC, the Oliver North Show, Mary Matalin Show, Beverly LaHaye Show, Janet Parshall Show, Dick Staub Show, and the AFA national radio network.

Before creating the Institute, Scott was a stockbroker and financial advisor for fourteen years beginning with E.F. Hutton. As a financial adviser, Scott was an active public speaker as well as a guest lecturer on cruises. Scott was also involved in the media a financial adviser. He hosted his own weekly radio show and was a daily commentator on business for the local CBS-affiliate morning television news in Washington state.

Scott earned Bachelor degrees in economics and political science at the University of Idaho where he was Student Body President. He also studied finance in graduate school at the University of Houston.

Scott has been involved in his local church at various levels including as a Sunday school teacher and board member. Scott is married to the former Joan Bramon of Sun Valley, Idaho. They have three children -- Rainer, Spencer and Lexington -- and live in Herndon, Virginia.

Testimony of
Scott Fehrenbacher,
Vice President of Crosswalk.com, Inc.
Before the
Commission on Online Child Protection (COPA)
Hearing on
The impact of Filtering, Rating, and Labeling on Content Providers

July 20, 2000

Mr. Chairman, Co-Chair Vradenburg and Co-Chair Hughes, and Honorable Members of this Commission, thank you for the generous opportunity to testify this afternoon to discuss the impact of filtering, labeling and rating on content providers.

It is an honor to speak to the commission today on behalf of the effort to protect children from the unfortunately abundant poison available on the Internet. As Vice President of Crosswalk.com, the nation's largest Christian Internet community site, I am responsible for the development of content programming and delivery for over a dozen channels of topical programming. Overseeing the work of multiple channel editors as well as in-house and independent writers, this responsibility includes making both long term policy decisions and daily decisions in conjunction with my editors regarding appropriate story themes, words, phrases or quotes.

Each day, we deliver fresh news, features, newsletters, and unique applications to our niche constituency. Our audience depends on a firm, accurate and consistent standard in delivering this varied information. In fact, our core audience can be generalized as being very cautious, perhaps even fearful, of the negative impact the Internet can have upon their families.

In this environment, my company has taken an aggressive advocacy role for the use of filtering as a tool for families in their effort to safely invite the Internet into their homes.

My company actually chose to be among the first to offer server-side filtering available for free. We believed that filtering would strategically make our product better, safer, and more attractive to the consumers we were trying to attract.

In defining boundaries with our filtering partner, we chose to focus on filtering out content that included: (1) sites labeled as "adult only", (2) sites advocating, promoting, or giving advice on carrying out acts widely considered illegal, (3) sites containing pornography, violence, sex or nudity, (4) advocacy of the recreational use of alcohol or controlled substances, and (5) information on the use of weapons or weapon making.

Cost was a factor. While the company did absorb significant costs in delivering a free filtering solution directly to our customers, we tactically believed that the value it represented to our audience would deliver both a financial and cultural return on investment from a growing market share and from loyal members generating increased traffic to our site.

From a customer service perspective, the company must educate our members of the values and limitations of filtering as well deliver customer service to support the filtering mechanism. This represented a great deal of man hours in initial development as well as significant man hours of labor each week for support.

In the day-to-day delivery of our content, all writers and editors at my company must be aware of the filtering standards in place. We have even had some of our own stories inadvertently filtered out along the way as the editors learned how to work within the standards in cases such as medical terminology activating a filter block.

Overall, the process of creating a broad spectrum of daily content to our audience within the boundaries of our filtering definitions has been quite manageable for our writers and editors. In the process, there has been no evidence that these boundaries have compromised the quality or accuracy of any content that has been created for our audience.

In searching for any collateral negative impact on the user experience of our members, we found very few substantive complaints about any performance problems in the speed of downloading our pages due to our filtering programs. Over time, the filtering solution we created matured to a level of sophistication and integration with our content servers that performance standards were maintained.

I join my company in remaining a firm advocate for the use of responsible filtering as an effective tool for parents in harnessing the immense value the Internet represents to their families while minimizing its inherent risks. In continuing to promote filtering as a solution to making the Internet safe, I believe that there are a few major barriers to overcome.

Historically cost has been a major factor in limiting the widespread adoption by families and public facilities. As with many other sectors of the Internet business, the costs of this service have declined dramatically in the past two years. In fact, the costs of filtering today have actually fallen to zero with some providers.

Other issues I believe have impeded the use of filtering include:
Poor performance – the results of the product were, or were perceived to be, inadequate and ineffective in measuring up to the promise of actually filtering out pornography and harmful content to children and families.

Electronic drag – many filters slowed the loading of pages and provided a poor user experience ultimately ending up in abandonment of the filtering system.

Education – A large percentage of users do not recognize the availability of low-cost or free filtering solutions that are dependable in delivering the protection they promise. The marketplace will play a significant role in broadcasting this knowledge to the public which should result in a larger segment of the population integrating filters with their Internet service.

Like filtering, content labeling using systems such as PICS (Platform for Internet Content Selection) was originally designed to help parents and teachers control the content that became accessible to children. However, as a content provider, labeling can potentially create a much more labor intensive and costly burden. In my position, I find little motivation to add a new level of individual standards and tags for my editors and writers to consider and manage when crafting new content for our members.

Beyond the black and white standards involved in filtering solutions, I fear that labeling has the propensity of leading to much more subjective definition boundaries. What my editors label as content suitable for teens but not children may not be consistent with label decisions made by other websites. Besides the potential for inconsistent standards, labeling can lead to an Internet ratings system ripe with the same shortcomings and weaknesses that the television networks have met with their attempt at creating six rating categories.

For example, besides the two children's categories the television networks have agreed to create, the ratings system includes "TV-G," "TV-PG," "TV-14," and "TV-M" ratings. With their age-based approach, these network ratings actually conceal what kind of objectionable content prompted the ultimate rating. There is no way for a parent to know if the rating was due to violence, profanity, sex, or all of the above. As another example of the confusion these ratings have created, the *Washington Post* recently quoted a 12-year-old girl in an interview regarding the ratings system. The girl said, "I read that 'TV-G' stands for 'Too Vague, Parents Give Up.'"

The explosive growth of pornographic and obscenity distribution on the Internet is terrifying to me personally as a father and professionally as a part of the Internet community. From the perspective of a content provider with a large audience, I believe the solution begins with an accessible, affordable and effective tool to empower Internet users in protecting their children from harmful material. Such a solution must also incur minimal burdens upon the shoulders of content providers as measured in time, technology and labor costs.

Significantly, content providers are just now experiencing the significant burdens of increased staff requirements and technology monitoring regarding the new regulations implemented from the Children's Online Privacy Protection Act. According *to Internet World* magazine in its July 15, 2000 issue, one website (Zeeks.com) has recently had to add three full-time employees just to handle the permission slips that come in every day from parents who want to give children under 13 access to their site. Of course, this is to conform to the new regulations as defined in the legislation. Solutions that burden content providers substantially may decrease the effective implementation of the laws and may also inhibit the value of the Internet itself.

As a content provider, I fully endorse and support the mission of the Commission on Online Child Protection as well as the obligation of the United States government to fully uphold the existing obscenity laws and prosecute those who choose to break them. In addition, I look forward to embracing new solutions and technologies that are part of the solution to protecting the children of America from the destruction of pornography.

Thank you for the opportunity to testify this afternoon to the Commission.

Eric Aledort
Vice President for Corporate Development/Government Affairs
Disney's Go.com

Eric Aledort is Vice President for Corporate Development/Government Affairs for Go.com, the Walt Disney Company's internet division. Eric previously was Vice President, E-commerce business development and V.P. business and legal affairs. He has been with the Walt Disney Company's internet group for four years and has taken a lead role in policy with a focus on privacy for children. Eric attended Georgetown University Law Center.

TESTIMONY OF ERIC ALEDORT
VICE PRESIDENT, CORPORATE BUSINESS DEVELOPMENT AND GOVERNMENTAL AFFAIRS
DISNEY'S GO.COM

BEFORE THE

COMMISSION ON ONLINE CHILD PROTECTION

JULY 20, 2000

Eric Aledort
Vice President, Corporate Business Development and Governmental Affairs
Disney's GO.com
5200 Lankershim Boulevard
Suite 413
North Hollywood, California 91601-7565
(818) 754-7150, Telephone
(818) 754-7205, Facsimile

Good afternoon, Mr. Chairman and other distinguished members of the Commission on Online Child Protection. I am honored to appear today before your Commission as it examines the protection of children through Internet filtering, labeling and ratings. I am Eric Aledort, Vice President, Corporate Business Development and Governmental Affairs, for Disney's GO.com, the online business unit of The Walt Disney Company. Disney's GO.com includes, among other things, ESPN.com, the most popular online sports site; Disney.com, the most popular online children's and family's site; and, ABCNews.com, one of the fastest growing online news site.

GO.com is committed to providing not only the very best online family entertainment but also a trusted and secure online experience. Online safety issues are, therefore, vitally important to us particularly as they pertain to children. GO.com believes that the following principles are critical to ensuring online safety. First, GO.com believes in educating kids and parents as to the dangers that exist online. Second, GO.com believes in equipping kids and parents with technological tools, like filtered search engines, to ensure safer online experiences. And, finally, GO.com believes in working collaboratively with content companies, online service providers, web sites, children advocates, parental groups, schools, policy-makers and international organizations to encourage self-regulatory best practices.

Go.com does not have a corporate position on the effectiveness of a worldwide Internet filtering, rating or labeling system. We are familiar with the efforts of the Internet Content Rating Association ("ICRA") and other groups. We understand the positions taken by First Amendment advocates, on the one hand, and children advocates, on the other. At GO.com, we are resolved to providing what's best for our customers, which is to say that GO.com feels that the Internet will best flourish if it's trusted and experienced by all. I would like to spend the remainder of my time and testimony, therefore, explaining specifically what we have done to provide our users with a safer online experience.

I. Education

In April 2000, we announced a comprehensive corporate policy requiring parents to provide credit card authorization prior to their children participating in any activities that involve external communications, such as message board posting, open chats, and holding an e-mail account. That same month, and in conjunction with a special television episode of "Disney's Doug" that explored the issue of Internet safety, Disney Online introduced Doug's Safety Web Page, providing families with an at-home resource for making wise surfing choices. The site features various interactive elements such as Doug's Top 10 Internet safety tips, Doug's Internet Safety quiz, a special edition of the "Ask Patti" Web page and more. In January 1999, Disney Online and the GO Network instituted a registration system requiring children under 13 to obtain parental consent prior to participating in online activities in which participants must provide personal information.

II. Technology – GOguardian

In January 1999, we launched the unique filtering software GOguardian, which helps our users control access to adult content on the Web. When activated by a user, GOguardian blocks adult queries and filters out adult content from the Web index. The result is a highly relevant collection of quality sites – those free from material that might be offensive to users or inappropriate for children. GOguardian can be turned on from every search box and is automatically turned on when for registered minors at our network of sites.

We are particularly proud of features of GOguardian such as the password-protection tool for maximum security. Through this feature, parents can "lock" Goguardian on to ensure that no adult-related search is performed without their consent. There's the "warning screen" feature that appears any time an adult-related search is performed – regardless of whether GOguardian is activated or deactivated. The warning screen alerts users that they may be inadvertently receiving adult content in response to their search request. The screen gives them the option to return to the search box or to continue in the activity. Another feature of GOguardian is the implicit assumption it makes. The GO search engine assumes you are not looking for inappropriate adult material.

At GO, we take the benign meaning of search terms rather than their implied adult-related meanings. An example we often use is the word "cheerleader," which when entered into our search engine results in sites on legitimate summer camps and collegiate teams. The same word when entered into other Internet search engines pulls up sites connected to pornography. In our Kids Center on GO.com, the GO Network provides links to a variety of Internet filtering software, such as NetNanny.

GOguardian protects our users – of all ages – from pornography in that it blocks sexually-explicit terms. Search queries using those terms will return with no hits. We operate GOguardian over a sub-set of the index of words and terms that are non-pornographic. Finally, we routinely eliminate spamming sites from our main Web index. Pornographic sites are not permitted to send spam to GO users and will not be permitted to appear in our search results. We are, thus, constantly updating our site database to screen out sites with objectionable matter.

III. Industry-Wide Initiatives

In July 1999, Disney Online became a founding member of GetNetWise, a web-wide online safety resource for families and kids. We have dedicated a permanent home for safety on our own web sites. Disney Online's Internet Privacy Policy and Internet Safety Information is available from every page of our

Network. Simply put, GO.com feels that kids and parents should always have safety resources that are one-click away.

In September 1998, Disney Online participated in the America Links Up campaign, which brought together educators, public, private and non-profit organizations in a public awareness event designed to help kids, parents, teachers and others learn how to use the Internet safely and productively. In support of this cause, Disney Online produced two informative public service announcements that ran on numerous broadcast and cable outlets designed to encourage kids and their parents to surf the Web together.

In March 1998, Disney Online hosted its first "Smart Surfing Week," an education program dedicated to helping families navigate the online world wisely. Tying-in with a provocative Internet safety episode of Walt Disney Television's "Smart Guy," Disney Online presented live, moderated chats with Tahj Mowry, the 11-year old star of the show, and two LAPD officers focusing on the lessons learned on the television show.

In December 1997, Disney Online published the CyberNetiquette Comix series, which provided families with an entertaining and interactive way to learn valuable lessons about online safety. Each episode of CyberNetiquette Comix, such as "Who's Afraid of Little Sweet Sheep?" featured The Three Little Pigs, was designed for families to first explore together and then discuss.

IV. Conclusion

In conclusion, Mr. Chairman, we feel that the task before us of protecting kids from inappropriate material online is a daunting one. No one solution – be it technology, legislation or education – will work if it is not part of a coordinated effort. The Internet is simply too large and sophisticated a medium for such a singular solution. There is no silver bullet. Rather what is required is a broad-based effort to educate and equip children with the means to find and then stay within the trusted spaces of the Internet. At The Walt Disney Company, we pledge to lead that effort.

Thank you and I would be pleased to take any questions.

David Biek
Tacoma Public Library

Mr. Biek has served as a public services manager at the Tacoma Public Library since 1988. In 1995, he became the manager of public services at the Main Library, the central facility for the 10-branch system. In that capacity, he helped design and implement public Internet access for the Library and has day-to-day responsibility for the public access systems and policies. Before coming to Tacoma, Washington, he held positions in the Solano County and Shasta County Libraries in California.

He received both his Bachelor of Arts degree in Anthropology and Master of Library Science degree at the University of California, Berkeley, the latter in 1975.

Testimony July 21, 2000

David Biek
Main Library Manager
Tacoma Public Library

Internet Use at the Tacoma Public Library: Our Findings and Experience

Background

Very few data exist that describe the people who use Internet services in public libraries.

Although controversies have reigned over Internet services in public libraries, especially with respect to children and pornography on the Web, the only demographic information about Web users that does exist is has been derived from user surveys and anecdotal accounts. The key question – To what extent do children in public libraries find pornography on the Internet? – cannot be answered from without actual user data.

My aim in testifying before the Commission on Child Online Protection is to share the data that we have collected at the Tacoma Public Library that bears upon this question.

One reason we wrote our own Web browser, which we call Webfoot, was to be able to design exactly the reporting system we wanted. As a consequence, we are able to collect statistics that no commercial browser software can deliver. The Appendix explains in more detail our decision to write our own browser.

This paper offers data collected in the course of day-to-day use of the Internet in all ten branches of the Tacoma Public Library, covering the period from October 1, 1999, to June 30, 2000. The data exist because each Internet user during that period, as a part of the login process, was required to enter his or her library card number as a password.

When a Tacoma Public Library card is used, whether to check out materials or to sign on to the Internet, the automated system logs certain non-identifying demographic information that is a part of each library card record: year of birth, gender, and census tract of residence. (No information is released in violation of the Washington statute protecting library patron confidentiality. The Library validates the patron data once each year to ensure that address or other changes of information are recorded.) Data pertaining to the Internet session itself is also logged, including the terminal number, the branch location, the time of day the session began, the length of the session, and characteristics of the session itself, including pages loaded, pages failed, and URLs entered.

We can compare data from the United States Census, the Tacoma Public Library circulation system, and the Webfoot Internet browser to analyze how Internet use might match or might differ from other library uses for which a library card is required. Correlating these data sources helps us answer the question, voiced often by public librarians in the Internet era: "We're busier than ever and checking out no books!" We can also compare our data, on a census tract basis, to see how representative of city residents as a whole library users and Internet users might be.

In deciding to offer public Internet access in the Library, the Board of Trustees was aware that pornography and obscenity were issues to be dealt with. The Board decided, in essence, that graphic material of the sort described in the State of Washington "harmful to minors" law was no more suitable on Library computers than they would be on billboards on city streets.

Here's the relevant passage from the Board policy:

> The Library's acquisition of Internet materials to be made available to Library patrons does not include graphic materials depicting full nudity and sexual acts which are portrayed obviously and exclusively for sensational or pornographic purposes.

The Library's full Internet policy may be found at <www.tpl.lib.wa.us/v2/using/net.htm>

The Library's implementation of filtering software is unique. **No website is blocked and all text is delivered.** The emphasis in the Board policy is upon **images** ("graphic materials"). When the CyberPatrol software detects a site on its lists in the "Sexual Activity" or "Full Nudity" categories (the only categories we implement), Webfoot takes over and offers the user a choice to connect to the site with the images inhibited from display. All the text is presented, with the image files are represented by placeholder icons. Webfoot also meets our requirement that user feedback be made as easy, comfortable, and speedy as possible, by popping up an email message box for the user should he or she wish Library staff to review the filtering of the site.

Findings

During the survey period, public Internet access was provided at 184 terminals. A total of 56,743 user sessions were recorded and almost 7,000,000 web pages were loaded. In the tables that follow, "Web Sessions" is a count of unique user sessions. "CyberPatrol Sessions" shows the count of user sessions in which at least one CyberPatrol filter intercept was encountered; there were 3,556 CyberPatrol sessions over this period, 6.2% of the total sessions. The "City Population" is the

1999 estimate and the figure for "Circulation" is the total circulation for all library materials in 1999.

Gender

	City Population	Circulation	Web Sessions	CyberPatrol Sessions
Male	48%	41%	63%	75%
Female	52%	59%	37%	25%

Most observers of Internet phenomena would say that men and boys far outnumber women and girls at the terminals. Our data support this. At the same time, females are a slight majority of the population of the city of Tacoma and a significant majority of those who check out library materials.

On the Web, the ratio of male to female Web users is reversed, and then some. Even more extreme is the preponderance of males when sessions involving CyberPatrol intercepts are involved. The Internet has, plainly, brought a new male audience in to the library.

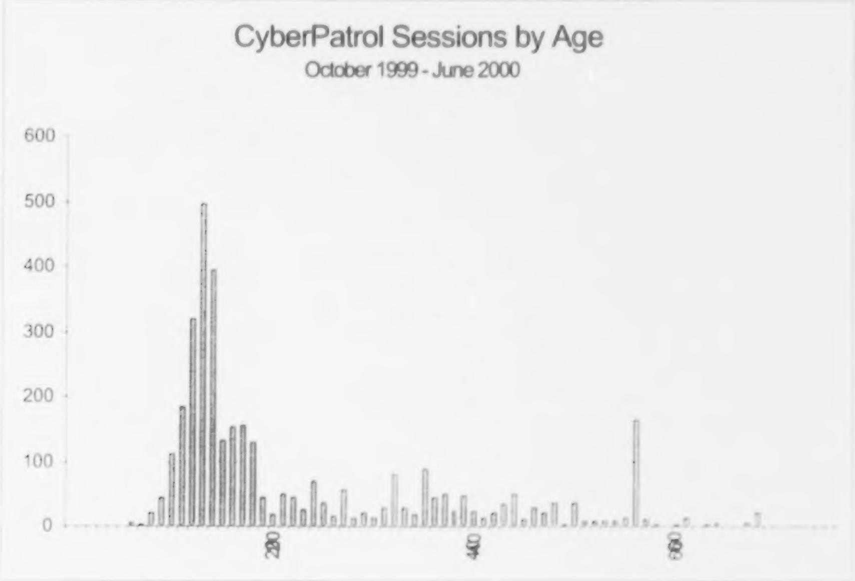
Age

	City Population	Circulation	Web Sessions	CyberPatrol Sessions
0-04	8%	0%	0%	0%
05-14	14%	17%	27%	44%
15-24	15%	16%	19%	23%
25-34	19%	17%	15%	9%
35-44	15%	21%	19%	11%
45-54	9%	15%	12%	5%
55-64	7%	7%	5%	6%
65-74	7%	4%	2%	2%
75+	7%	3%	1%	0%

Median	32	34	27	16

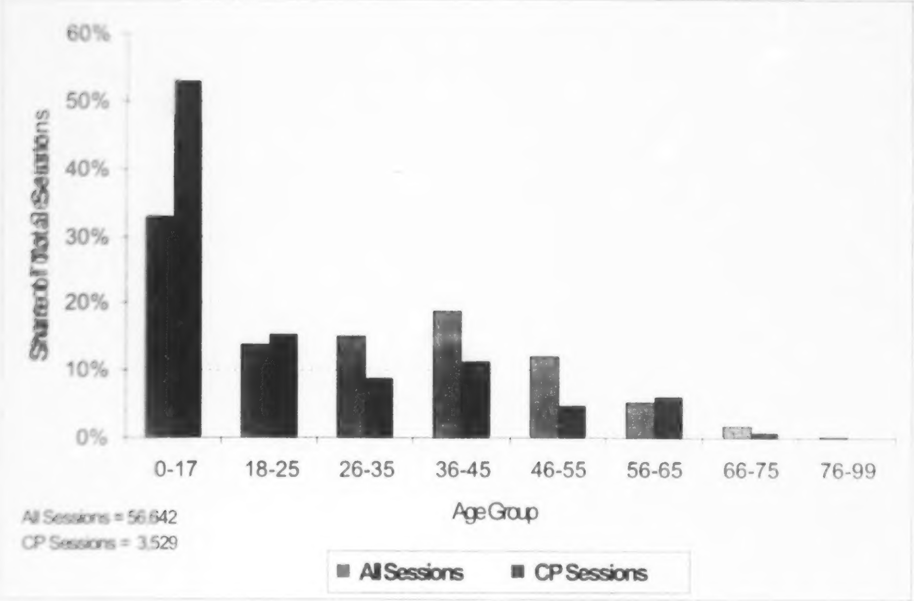
There is a reasonably good match between library card use and the population of the age group. The median ages of these two groups are also close to the same, 32 and 34 years, respectively. Web users are markedly younger, with a median age of 27. Close to half of all Web users are between 5 and 24 years of age.

The most startling finding is that users who register at least one CyberPatrol intercept during a session are so much younger than Web users in general. The median age where CyberPatrol intercepts are involved is just 16 and the single age most frequently seen is 13.



A person 17 years of age is considered to be a minor in the State of Washington, and so the age data may be aggregated to show:

	City Population	Circulation	Web Sessions	CyberPatrol Sessions
0-17	26%	23%	34%	57%
18 +	74%	77%	66%	43%



The next chart presents that data in more detail:

In recent months, reports have included cross tabulations for gender and age. The same picture is seen for boys and girls: the 10 to 17 age group for each sex accounts for the majority of filter activity.

	Male		Female	
	Sessions	CP Sessions	Sessions	CP Sessions
0-17	36%	63%	36%	70%
18-25	10%	8%	13%	7%
26-35	13%	3%	15%	6%
36-45	23%	12%	15%	8%
46-55	10%	6%	16%	7%
56-65	5%	7%	3%	2%
66-75	1%	0%	2%	0%
76-99	0%	0%	0%	0%

A major theme of the Internet policy of the Tacoma Public Library is stated terms of the protection of minors. The data show that the concern of the Board of Trustees in setting this policy was well founded.

Census Tract of Residence

The City of Tacoma comprises 39 census tracts. Our patron registration process automatically assigns a census tract to each patron record based upon the residence address. Analysis of the web activity data is suggestive but highly tentative, since we suspect that the year 2000 Census of the city will show significant demographic changes from the 1990 census.

We do think that the year 2000 information will show that neither total Web sessions nor CyberPatrol sessions are strongly correlated with census tract population numbers. Rather, we believe we will find stronger correlations between: 1) web usage and median age and educational levels, and 2) CyberPatrol intercepts and median age and income levels.

Effectiveness of the Library's Internet Implementation

One reason the Tacoma Public Library chose CyberPatrol was that the software provides an easy mechanism for system administrators to override the website addresses set by the producer. What we expected, and what we have found, is that modifications have indeed been necessary.

We implement two of the CyberPatrol categories: "Sexual Activity" and "Full Nudity." Because of the highly circumscribed requirements of our Internet policy, some sites that are correctly listed according to the producer's criteria should not be flagged on our Library terminals.

The major reason for this is that these sites do not include illustrations of a nature prohibited by Library policy. These may be sites featuring text-only erotic or pornographic stories, adult personals ads, collections of dirty jokes, sites with music lyrics that merit "parental advisory" warnings, sites featuring photographs of women in bikinis or skimpy wrestling apparel not involving nudity, and "warez" sites which include cracked triple-x passwords. These sites are added to the override "allow" list. We learn about sites such as these through user feedback and my own review of the system logs.

Recall that when a site flagged by CyberPatrol is encountered, the user is presented with an email form that can be used to request that the Library review the site. This is analogous to the process we have always offered library patrons for the reconsideration of books in the collection. The form may be submitted anonymously or the user may choose to include contact information for a reply. I review each of these requests and aim for a 24-hour turnaround in my decisions.

Over the period of time described in this study, our users have submitted 1,153 of these requests. In a typical month, 85% of them are from sites, which do indeed include image content that violates Library policy. Almost all of the rest are correctly flagged according to CyberPatrol's category definitions but fail to meet the more strict requirements of Library policy. These are added to the override list. A few each month do not appear to me to meet the software producer's own definitions; these are also added to the override list and we take the extra step of notifying the company of the problem.

The second source for modifications is my own review of logs of filter intercepts. I check any URLs that I do not recognize as correctly flagged and take appropriate actions. Typically, 95% of all the URLs listed in these logs are properly treated by our system.

The result is that the software list of flagged sites is constantly refined and improved.

Comments on the Library's policy and procedures from members of our community have, with a bare handful of exceptions, been positive and supportive. Some of these comments have been made in connection with well-publicized incidents involving neighboring library systems and Internet pornography.

Conclusions

Month after month, we find that about 6% of all sessions at public access Internet stations at the Tacoma Public Library involve websites flagged by the filtering software. That sounds like a small number, but when the number of sessions is large (now about 7,000 per month and growing), then the number of incidents in an unfiltered environment would be intolerable.

But it could be worse. That 6% is in an environment where a filtering procedure is in place. If nothing were in place, then we would expect the number of incidents to be much higher.

We know that the majority of filter incidents involve minors, with a significant share involving 13 and 14 year olds. Our experience says that the stereotyped "dirty old man" is not looking for Internet pornography at our library.

At the same time, the unique implementation at the Tacoma Public Library ensures that users are able to access any URL on the web and that all text at a flagged website can be delivered.

User satisfaction and community acceptance are high and an efficient mechanism for user feedback is in place.

The Internet has brought a new audience to the Tacoma Public Library. With solid numbers, we can show our governing Board of Trustees how Internet services, in the context of public library service, are used. The information also helps us to craft policies and procedures to ensure that these new services are provided in an effective and responsive manner.

Appendix

Why the Tacoma Public Library Wrote Its Own Web Browser

We began investigating browser software in 1996, at a time when Lynx was the only browser available at the Main Library for the public. Lynx is a text-only tool, difficult to use and to teach.

Mosaic and Netscape were the major commercial browsers available, although Internet Explorer was by then becoming a serious contender. We found that none of these commercial products could deliver even a fraction of the features we wanted.

It's important to emphasize that Internet implementation at the Tacoma Public Library began with many discussions among staff, administration, and the Board of Trustees about the way that Web-based information fit in with the Library's overall service plan and sense of mission. Building upon that, we attempted to build the best possible hardware and software suite to implement these local decisions. The situation, of course, is fluid, and our system has evolved to meet user needs and new technical possibilities.

We had five goals that could not be achieved with a commercial browser:

- We needed a way to control printing costs.
- We wanted to gather reliable statistical information.
- We knew that a number of issues related to browser use by neophytes would need to be addressed.
- Based upon our experience in providing a computer lab in a public library setting, we knew that security and user privacy had to be ensured.
- And, we knew we had to fix obvious deficiencies with available filtering software in order to implement the Library's policy of inhibiting certain graphics from display.

In the years since 1997, when Webfoot made its debut at the Main Library, the commercial browser market has shaken out, leaving Internet Explorer dominant, with Netscape also a major player. Neither of these products, however, is any closer to offering the feature set we desired.

Printing Control

Users have two options for printing from the Web. (They can also save files to floppy discs and can send data to any valid email address.) A text-only print can be made at the ink jet printer alongside each terminal. These prints bear a statement telling the user the amount due for the print. Payment is on the honor system.

Text with images or any degree of formatting, however, is better done on a laser printer. If a user chooses the laser print, the local printer produces a small ticket that shows the price of the print (at ten cents per page) and the job number in the laser printer's queue. We print the required material only when the user has decided to pay for and take the material. We save money on printing since nothing is printed (except the ticket) without being paid for to recover costs. Users are served well, too, since they incur no costs until they are sure they do want the printed material.

Statistics

Web surfing only seems free of cost. In fact, every library that provides Internet access incurs major costs. Rarely are new, untapped sources of funds available to provide the service. Detailed usage reports are the only reliable and objective way to ensure that the Library's investment represents value to the community.

By writing our own browser, we were able to design exactly the reporting system we wanted and therefore we are able to collect statistics that no commercial browser software can deliver. For each public terminal, for each library branch, and for the system as a whole, we have counts of:

- hours of use
- user sessions
- pages loaded
- page loads failed (and the reasons for the failures)
- the occurrences of CyberPatrol flags
- various user commands issued
- downloads and printing activity

° uses of the Library's own website

Because users enter their library number of begin a session, we can collect aggregated demographic data, including age, gender, and census tract of residence.

Ease of Use

Webfoot is not an elaborate piece of software. Consistent with the Library's purpose in making the Web available, the feature set provided is the minimum necessary for efficient web-browsing. We also wanted a browser that would be easy to learn to accommodate the technophobic element of our public. For example, Webfoot has de-emphasized the need to use a mouse by providing keyboard shortcuts for many frequently performed operations.

Security and Privacy

At the time Webfoot was written, Web users in a shared environment such as a public library faced risks to their privacy. Identifying information related to a user's web session was recorded in a number of places, including the cache, history files, settings files, and cookies. With little difficulty, the following user could have access to this information. Webfoot automatically clears or deletes these files at the end of each session.

System security in a shared environment was also a concern. By 1997, the Library had ten years' experience operating a Computer Lab - eight personal computers in a network for word processing and similar uses. We knew from this experience that we could expect vandalism and mischief from hackers at the Internet stations. Webfoot includes many design features to protect the Library's networks. The "clearing" done at the end of each session also reduces security risks.

Webfoot and CyberPatrol

When we began to design Webfoot, web-filtering software had advanced beyond crude word blocking but the state of the art still left much to be desired. We were not willing to accept the only outcome that filtering software then available could deliver: that is, a site that was on the software's list of URLs was absolutely unreachable. Furthermore, mechanisms for users to request reconsideration of blocked sites were not integral parts of the filtering software systems. We also wanted to be able to override the software as needed by adding to or deleting from the list of sites without imposing on staff too heavy an administrative burden.

From our experience in a text-only Lynx environment we knew that our users were not be reluctant to seek out pornographic materials on the Web and we expected that such interest would be much greater when the graphical browser was introduced. In the new graphical environment we wanted only to inhibit the display of those particular images which were not allowed under our Board policy for Internet use.

Following close scrutiny of the software filtering products then on the market, we selected CyberPatrol. In this program, the lists of URLs are categorized so that we were able to approach our policy goals by selecting just two categories for implementation; so-called word blocking is not used. Overriding the software is easy for our system administrator to do. Finally, we saw that we would be able to write the Webfoot software so that the literal and exact purpose of our policy could be achieved.

When a user requests a site that appears on one of the two CyberPatrol category lists, Webfoot intervenes to explain that the requested site has been flagged by the filtering software and asks the user whether he wants to see a text-only version of the site. If so, then the requested site is displayed, with small placeholder icons replacing the. No text at the site is blocked.

Webfoot also meets our requirement that user feedback be made as easy, comfortable, and speedy as possible, by popping up an email message box for the user. Staff review is expedited since the email message contains the URL of the site; clicking on it in an unfilte

Web Use at the Tacoma Public Library

7/18/00

Click here to start

Table of Contents

Author: DavidB

Web Use at the Tacoma Public Library

Web Use at the Tacoma Public Library

Web Use at the Tacoma Public Library

Web Use at the Tacoma Public Library

Web Use at the Tacoma Public Library

Web Use at the Tacoma Public Library

Web Use at the Tacoma Public Library

Carolyn Caywood
Librarian
Virginia Beach Public Library System

Carolyn Caywood has been a librarian for 28 years, the last 20 in the Virginia Beach Public Library System. Since 1984, she has managed the Bayside Area Library in that system, but she considers herself to be primarily a youth services librarian and wrote a column on teen library services for School Library Journal from 1990 through 1998. She is a graduate of Wayne State University and a member of the Freedom to Read Foundation Board, the American Library Association, and the Virginia Library Association. Locally in 1993, she helped found a public user group, the Hampton Roads Internet Association, which still meets at the library.

Public Access to the Internet in Virginia Beach

submitted by Carolyn Caywood, Virginia Beach Public Library

July 21, 2000

Located in the southeastern corner of Virginia between North Carolina, Norfolk, Chesapeake Bay and the Atlantic, Virginia Beach is part of the Hampton Roads Metropolitan Statistical Area. It's the largest city in the state and the 34th largest city in the United States. Also the fastest growing city on the East Coast, it is expected to surpass 500,000 by the year 2010. The city covers 310 square miles, including 156 farms and has approximately 32,700 acres of land under cultivation. Virginia Beach is home to four military bases employing 32,000 armed services and civilian workers. The city's popularity as a tourism destination brought 2.5 million visitors in 1997. For more background, see http://www.virginia-beach.va.us/dept/econdev/background.html.

That page adds, "As the first recipient of the American Society of Public Administration (ASPA) National Innovation Recognition Award, Virginia Beach government was cited for excellence and innovation in organizational development, strategic planning, quality initiatives and process improvements. The award recognized Virginia Beach for successfully changing its organization to improve local government, be more competitive and more citizen and customer focused."

One expression of this focus is Virginia Beach, Virginia, Community for a Lifetime: A Strategy to Achieve City Council's Vision for the Future which guides the development of government policies and services. On page 17, City government expresses the belief that, "Individuals form the foundation of any society. If individuals are competent and confident and have support and resources, they can take responsibility for their own lives and reach their full potential. Families form the first level of support for individuals. Therefore, families are the primary force in shaping lives and developing positive experiences and healthy relationships."

In the early 1990s before most people were aware of the Internet, Virginia Beach, like many other cities, had the problem of city government facilities being used as day care substitutes. The affected government departments worked together to create both a policy and a public education initiative. Their objectives were:

To assure the safety and welfare of unattended children.
To develop communication among staff, parents, and children.
To facilitate cooperation and communication among City agencies, including the Police Department and Social Services, having responsibilities concerning unattended, neglected or potentially (or seemingly) abandoned children.
To conserve staff personal resources.
To deter the use of public libraries and recreation centers as ad hoc child care facilities

Since the policy, Unattended Children in Libraries and Recreation Centers, was adopted Jan. 31, 1996, its enforcement provisions have never been exercised in the libraries. Educating families on the legal and safety issues has proven fully effective and government confidence in informed parents has not been misplaced.

This philosophy has guided the Virginia Beach Public Library as it provides services through a Central Library, six branches, a bookmobile, and three specialized libraries. In addition to a staff of 202 FTE, volunteers contribute 25,794 hours to library operations. The collection contains over 800,000 individual items which were checked out 2,777,075 times during 1,585,513 visits last year. The website http://www.virginia-beach.va.us/dept/library/ gets over 400 different visitors per day from users outside the libraries. With the help of a Gates Grant, there are now 94 public computers with Internet access.

The library approached the Internet through dialog with the community. A first step was to sponsor a public user group, the Hampton Roads Internet Association, http://www.hria.org/ in late 1993. Library staff presentations to the group included a discussion on filtering and blocking software in 1996. http://www.pilot.infi.net/~carolyn/guide.html. Less technically minded citizens were also consulted --187 participated in a series of public dialogs in 1997 on the future of the library. Book displays, classes and interactive programs have allowed staff and public to exchange views on Internet issues ranging from safety tips to evaluating information quality. All of these contributions have helped shape how we offer the Internet.

As the library developed its plan for public access to the Internet, other city departments were consulted. We worked particularly closely with law enforcement, including the Police, the Sheriff's office, the City Attorney, and the Commonwealth's Attorney. The Library Board reviewed the plan as it developed. Central to our planning was the City government strategy, "We treat people primarily as individuals with capacity rather than individuals with needs, in our relationships with the citizens of our Community and the members of our organization." p.19. We have assumed that the library's role is to teach, assist, and facilitate the development of information literacy skills and that the people of Virginia Beach have the capacity to employ those skills to make their own decisions in using the Internet. We believe the best guide for children in using the library, the Internet, or indeed any source of communication and information, is their own parents. This has led us to focus on offering informed choices. For the youngest users, we have Kidsnet which is a small collection of websites selected by library staff for their developmental appropriateness for children through age eight. Older users can choose between Internet workstations filtered by I-Gear and Internet workstations that are recessed to prevent casual invasion of privacy. Each workstation presents the library policy with an I AGREE button for further access. Chat is not supported on any library workstations. Signs explain the different workstations and handouts address frequent questions. E-volunteers supplement staff in teaching new users and maintaining order.

Virginia Beach, Virginia, Community for a Lifetime: A Strategy to Achieve City Council's Vision for the Future summarizes on page 3, the Roles of Government. "In the past, we focused on providing services as the main way to carry out our mission. Today, as a result of our planning, we realize that we must emphasize three dimensions of service in order to succeed. They are:

- To provide municipal services which are valued by citizens,
- To provide information and knowledge to enable Community success,
- To ensure that things happen, by being a catalyst, mobilizer or facilitator."

We believe that public access to the Internet as provided in the Virginia Beach Public Library exemplifies the kind of municipal government service our citizens want for the future.

Appendices:

VIRGINIA BEACH PUBLIC LIBRARY
INTERNET USE POLICY
June 29, 2000

Acceptance Statement:

The Virginia Beach Public Library considers use of any public access computer in its facilities to constitute an acceptance of its Internet Use Policy. Customers will reaffirm the agreement each time they use the public access computer.

Background:

The Virginia Beach Public Library mission states:

> A literate populace and the freedom to read are essential to our democracy. The Virginia Beach Public Library system provides free access to accurate and current information and materials to all individuals and promotes reading as a critical life skill.

Free access only has meaning in a society that preserves freedom of expression. This freedom is protected in America by the First Amendment of the *U. S. Constitution*. The intentions of the First Amendment are at the heart of the Library's mission statement.

Court decisions over the years have interpreted the public library to be a "limited public forum." In such a forum, the government may not discriminate among constitutionally protected content or viewpoints. It may only regulate the time, place and manner of their use.

The information to which the Library provides access is increasingly available only in electronic form and over the Internet. The courts have found in recent cases that the Internet deserves the highest protection, because it broadens the opportunities for free speech. This decision puts the Internet at the center of the Library's mission.

The Virginia Beach Public Library endorses the principles of the American Library Association's *Library Bill of Rights* (http://www.ala.org/work/freedom/lbr.html), and its interpretation entitled "Access to Electronic Information, Services, and Networks." The

Library endorses the Virginia Library Association's "Intellectual Freedom Vision Statement" and "Open Access to the Internet" (http://www.vla.org/IFC/ifstatements.htm).

Responsibilities of the Library and its Customers

Librarians use criteria to select the materials acquired for the Library's collection. The Internet poses a different challenge. Its ever-changing resources are only partially reviewed and recommended. Users of the Internet must be aware that the content they access has not necessarily been verified for accuracy, currency or appropriateness. Library staff can recommend specific resources that have been found to be reliable and can offer advice on how to evaluate content.

The Library has designed and arranged its workstation furniture to assure customer privacy while using the Internet.

The nature of a public forum requires participants in that forum to exercise critical thinking skills to determine the truthfulness and relevance of the content they consult. In the case of minors, parents may need to supplement the inexperience of youth with guidance for their own children.

Service Plan

Internet Protocols

The Virginia Beach Public Library supports as many Internet protocols as it can, balancing security with access. The Library does not support the Internet Relay Chat protocol or provide assistance in using it, though we recognize that some websites will offer chatrooms anyway. IRC is the Internet protocol for synchronous, "real time" conversations on the Internet. This protocol is excluded as having little relevance to the Library's mission because:

The value of information communicated on IRC is diminished by uncertain authorship and lack of archival retrieval,

Other libraries report it is time- and resource-consumptive,

The pace of real-time conversation encourages ill-considered and unsafe behavior And, for that reason, it is the protocol most likely to be implicated in harm to young people.

Filters

At least one workstation, clearly marked, in each library agency offers filtering software for those who prefer to use it.

Library staff does not make any judgment about which workstation a customer should use. That decision is left to the individual user, or if the user is a minor, to his or her parents.

Children's Workstation

At least one workstation in each library agency is clearly marked for use by young children and their parents. This workstation enables them to experience selected Internet sites without providing access to the entire world wide web. The workstation is intended for children and their families to gain experience with computers and hypermedia in a limited and structured environment.

Time Limits

Each workstation has a set time limit for use, some short for quick lookups and immediate availability, and some longer for study. The workstations are clearly marked to indicate their time limits. Time limits are administered on an "honor system" among customers. They may be extended when there is no one waiting to use a particular computer.

Internet and Information Skills

The Virginia Beach Public Library provides a list of recommended links to help users develop safe and wise Internet skills. These links are reviewed regularly. They are available on the Library's website and in a printed form in each library.

Public Computer Lab

The Library provides training in Internet use and World Wide Web search skills in its Public Computer Room located in the Central Library. The Room also enables customers to use selected software products, and when classes are not in session, its workstations will be available as library workstations with Internet access. The use of the room is open to all library customers, regardless of age. A staff member is assigned to the room to guide the instruction in software use.

Law and Policy Restraints on Behaviors and Content

Some behaviors are not permitted in the Library's limited public forum. The Library has a set of behavior guidelines that apply to users of the Internet as well as to all other library services. In addition, customers are not permitted to:

change the settings and configurations of public access computers,
use non-library software or drives on library computers,
behave in a way that intrudes upon the rights of others. Customers are not permitted to invade the privacy of other library customers, harass library staff or customers, damage or disrupt library computer resources, or spam in violation of federal, state, or local laws or ordinances, including, but not limited to, *Code of Virginia* § 18.2-152 et seq.

Some content is not protected by the First Amendment to the *U. S. Constitution*. No library customer is permitted to use a library computer to view obscenity, child pornography, or to display this illegal content, or if a minor to view materials harmful to juveniles in violation of federal, state, or local laws or ordinances including, but not limited to, *Code of Virginia* §§ 18.2-372, 18.2-374.1.1, 18.2-390, 18.2-391, and 18.2-377. Nevertheless, the legal status of any particular content can only be determined by a court of law.

Library customers may not use library computers to violate copyright protection or licensing agreements in violation of applicable federal, state or local laws or ordinances, including, but not limited to, Title 17 of the *United States Code*.

Response to Prohibited Behaviors and Content

Library customers who encounter behavior that violates library policy should report it to library staff immediately. An individual who violates library policy shall be warned about the specific behavior that is prohibited. If the violation continues after warning, he or she may be banned from the facility for a specific period of time. If a user encounters behavior that may be illegal, either the customer or the staff can report it to law enforcement. Neither the staff nor the user can determine the legality of content -- only a court of law has that authority.

Adopted:

Date

Pat Deans
Chair
Public Library Board

Virginia Beach, Virginia Community for a Lifetime
A Strategy to Achieve City Council's Vision for the Future
p.17
Our Goal: Community: Building Relationships and Capacities
Individuals form the foundation of any society. If individuals are competent and confident and have support and resources, they can take responsibility for their own lives and reach their full potential.

Families form the first level of support for individuals. Therefore, families are the primary force in shaping lives and developing positive experiences and healthy relationships.

Virginia Beach is composed of many diverse communities - groups of people who share interests and beliefs (like religious communities), culture and heritage (like ethnic communities), a sense of place (like neighborhoods), or a common purpose (such as military, media, businesses, organizations, special interest groups and our own government community). For these communities to come together and be the Virginia Beach Community, caring and engaged relationships must exist among its individuals, families and communities. The Virginia Beach Community can accomplish things that individuals, families and communities can not do on their own.

We, the leaders and members of the government community, communicate and work collaboratively among ourselves and with the leaders and members of the other communities by:

- listening to understand our collective needs and values;
- adopting and realizing a common vision of Community that gives each of us a sense of belonging and caring;
- acknowledging and appreciating our considerable diversity and demonstrating and encouraging tolerance;
- building and modeling Community leadership;
- identifying and actively addressing the root causes of our individual and collective problems;
- creating and applying collaborative approaches and solutions;
- recognizing and growing individual and collective capacities to create and sustain our Community.

Unattended Children in Libraries and Recreation Centers

Index Number: AD3.10 Date of Adoption: 01/31/96

1.0 Purpose and Need

City staff at community recreation centers and public libraries regularly encounter situations in which children are left by their parents unattended for extended periods of time, both during and after the hours of normal operation. This Directive sets forth procedures to guide staff members when responding to situations involving such unattended children.

Implementation of this Directive shall be guided by the following objectives:

To assure the safety and welfare of unattended children.

To develop communication among staff, parents, and children.

To facilitate cooperation and communication among City agencies, including the Police Department and Social Services, having responsibilities concerning unattended, neglected or potentially (or seemingly) abandoned children.

To conserve staff personal resources.

To deter the use of public libraries and recreation centers and ad hoc child care facilities

...

3.0 Procedure to Accomplish Directive

III. Public Information and Training

The Department of Public Libraries and Department of Parks and Recreation will conduct an
ongoing public education program to inform parents of the need for appropriate preparation
and/or supervision of children who utilize the libraries and recreation facilities. The public
information program will include:

Coordination with the Public Information Office to promulgate Directive and its need through video announcements and press releases.

Placement of signs near each facility entrance, worded as follows:

PARENTS AND GUARDIANS ARE ADVISED THAT (LIBRARY) (RECREATION FACILITY) STAFF MEMBERS CANNOT CONTROL OR BE ACCOUNTABLE FOR INDIVIDUAL CHILDREN WHO ARE LEFT UNATTENDED ON THE PREMISES. IT IS THEREFORE THE PARENT'S OR GUARDIAN'S RESPONSIBILITY TO ENSURE EITHER THAT EACH CHILD IS ACCOMPANIED BY AT LEAST ONE PERSON OF APPROPRIATE AGE AND MATURITY LEVEL TO PROVIDE FOR THE CHILD'S SAFETY, OR THAT EACH CHILD IS ABLE AND PREPARED TO BE IN THE LIBRARY
ALONE.

Distribution of informative "checklists" and brochures regarding the unattended children Directive.

Alerting parents about this Directive on application forms when children are enrolled for library cards or for recreation programs.

Displaying posters with public safety messages related to unattended children and child safety in general.

From our class in cyberparenting

http://vbplitc101.homestead.com/files/parentbeyond.htm

Questions to consider to decide how much guidance an individual child currently needs:

Time -- does your child keep computer use in reasonable balance with other activities?
Privacy -- does your child know what information should not be given out?
Netiquette -- does your child know what behaviors are rude on the Internet?
Advertising -- does your child apply logic to temptation?
Misinformation -- can your child tell when content is biased or a hoax?
Skills -- can your child avoid undesirable content by using well-thought-out searches?
Values -- does your child know what you would want him or her to do in an unfamiliar situation?
Safety -- can your child recognize situations that might be risky?

Maturity -- will your child apply all this, in spite of peer pressure or curiosity?

Thoughts to keep in mind for both home and library use of the Internet:

Be involved. Surf online together -- parents and children can learn from each other. Understanding computers may seem easier for children, but you are better at knowing when to be cautious. Children need assurance that they will not be blamed if they tell a parent about an unpleasant encounter or ask for advice. If your child locates an objectionable website despite your precautions, sit down with him or her and talk about why you, as a parent, find it objectionable. Explain your values and what you expect of your child. *Library staff will not second-guess your decisions.*

Protect your privacy. Discuss what information is private in your family and how to handle situations where that privacy could be compromised. As a general rule, information that could allow someone to locate you should not be shared online. *The library does not keep any record of individual Internet use.*

Be skeptical. There are lots of rumors, mistakes, and outright lies on the Internet, so double check before you trust. Consider the other person's motives and credentials. The Internet is a great place to develop and practice critical thinking skills. *If you have concerns, library staff are experts in evaluating information.*

Be careful. When you know people online only, you don't really know them. Mistakes in Internet addresses can lead to unpleasant results, so don't guess. Make searches as specific as possible and add more words if the search results aren't what you expect. *Library staff can show you how to get the results you want.*

If you encounter something that makes you uncomfortable, delete it or back out of it. If a message doesn't feel right, don't respond. You can report child abusive material online to The National Center for Missing and Exploited Children, (1-800-843-5678 or http://www.missingkids.org/).

Be courteous and ethical. Don't copy someone else's work, and don't trust those who do. Don't insult people you disagree with. Don't forward rumors or send messages where they're not wanted. *Library staff can explain copyright, plagiarism, and netiquette.*

Interactive websites you and your child can use to reinforce these safe Internet practices:

For the youngest	http://www.familyguidebook.com/safesurfclub.html
Animated multiple choice	http://www.kidscom.com/orakc/Mousers/Internet/index.html
Animated characters illustrate lessons	http://disney.go.com/cybersafety/
Doug's Internet Safety Quiz	http://apps.disney.go.com/global/quiz/quiz.cgi?def=doug1
Get an Internet Driver's License	http://www.safesurfin.com/drive_ed.htm
Another multiple choice quiz	http://www.missingkids.com/quiz/internetquiz.html
Get a PBS web license	http://www.pbs.org/kids/did_you_know/did_techknow.html
Rocko's Safe Surfin' Trivia Challenge	http://www.nick.com/inits/safety/index.html
Ithaca College's Interactive Guide	http://www.ithaca.edu/library/Training/ICYouSee.html
Is it a hoax?	http://www.library.ucla.edu/libraries/college/instruct/hoax/evlinfo.htm
Evaluate web information	http://www.lib.calpoly.edu/infocomp/modules/05_evaluate

Carolyn Tuttle Roberson
Sr. Coordinator, Instructional Technology
Norfolk City Public Schools
800 East City Hall Avenue, Suite 800-A
Norfolk, VA 23510

Education

M.A.	The George Washington University, Washington, D.C.
5/1993	Administration & Supervision
B.S.	Longwood College
5/1975	Education

Teaching Experience

8/75 - 6/76	Northumberland County, Virginia Public Schools
	Classroom teacher
8/76 - Present	Norfolk City Public Schools

Classroom teacher, Helping Teacher, Teacher Specialist, Sr. Coordinator of Instructional Technology

The Consumer's Perspective
Testimony to the Commission on Online Child Protection
July 21, 2000

The introduction of the Internet into our schools and classrooms offers a genuine promise for improvements in teaching and learning. President Clinton's challenge to connect all of the nation's schools to digital networks has resulted in a revolutionary enthusiasm to make the school house a place where the "digital divide" can be conquered and students of all ages and backgrounds benefit.

With any change, especially wide-spread rapid change, come challenges of philosophy and pedagogy. In offering our students access to the World Wide Web, we have put them in reach of resources that have never before been available. The vast majority of these resources are pathways to subject matter that address local and state standards. School divisions such as mine require a parent/guardian and student signature on an "Acceptable Use Policy (AUP) for Internet Access." This policy states that web access has been established for access of information and research that enhances approved educational goals and objectives. Although our students pledge by their signatures on the AUP that they will not access material that is profane or obscene, that advocates illegal acts, violence, or discrimination toward other people, we, as a school system still feel an obligation to filter their access. Indeed, even before the Virginia Department of Education asked that schools provide filtering for students, Norfolk Public Schools had already made that determination.

Due to information that has been distributed by organizations such as *The National Center for Missing and Exploited Children*, our communities are aware of the pitfalls for child safety on the information highway. Again, due to communication directed at our constituents, Norfolk Public Schools has not received a great deal of objection from parents concerning the filtering and rating of our services. One local news station deployed a crew to Granby High School to attempt to foil our filtering process. Their attempts failed. Following the news broadcast our webmaster received feedback indicating that our customers were grateful for not only the blocking of harmful information, but also the blocking of information that has little to no bearing on our educational goals and objectives.

Could the filtering and rating technologies be construed as being in violation of First Amendment rights? Perhaps. Our concern is that educational web access is being used for appropriate educational purposes.

We, in the Hampton Roads area of Virginia primarily use server- or network-based filtering software that was introduced to us by former NASA "rocket scientists." Working closely with the Consortium for Interactive Instruction, this company offered a product that first met our initial needs and then allowed input for improvements. The product requires user authentication, enables us to customize our filtering list, and provides our webmaster the ability to create "allow lists." The filter, known as Dynamic

Document Review (DDR), is "real time" and examines the requested text in context and in multiple languages making a blocking decision based on the content of the page (that is what words are in proximity of other words) not just one or two words on the page. This allows for the safe use of search engines and pages not yet categorized. The DDR list is updated by a company specialist every 4 to 5 days and downloaded to our servers each time there is a change. The filtering can be tailored to meet the specific needs of every user, classroom, or grade level. Therefore, over-filtering is not the problem that it could be. A first grade class can have different access rights than a senior level or adult education class.

The software tracks each of the users on the network to ensure responsible use, and automatically "locks" a user's account when the locally specified forbidden access threshold is reached. In Norfolk schools that is three times. Not only does the district webmaster have access to student tracking information, but in our schools, a site-based manager will intervene when this threshold is reached. In addition, we receive e-mail notification from the filtering software company of an account "locks" and alerts. *(See attached examples.)* Parents are notified and students lose their privileges to use web-based resources. In order o regain their Internet privileges, students are required to complete a refresher course on appropriate use of the Internet and have a second AUP signed by their parent.

Although the use of student e-mail is limited in our district, Norfolk also uses a mail software that scans incoming and outgoing messages for inappropriate or objectionable content. It also gives the ability to specify where users may send and receive e-mail from. This feature protects our students from spammers and stalkers.

Within our school system's classrooms and libraries our children are recipients of the best protection that we know how to provide. In their homes, that may be another matter. We estimate that approximately 20% of our students have access to the Internet at home. Many Internet service providers have filtering options that need to be activated by parents. Family oriented "portals" have been established that offer filtering, free Internet service, and reduced pricing on home computers. We have no way of knowing whether our students are protected in their homes. Empowering and educating our parents, as well as providing access to inexpensive home filtering software that is user friendly could certainly keep our students safe while on the Internet at home.

In closing, I would be remiss if I did not mention that the Telecommunications Act of 1996 has brought schools affordable access to telecommunications. Even the most disadvantaged school divisions have been able to embrace computer/web-based learning and communications. This opens a whole new world to students and teachers. It is important that policy makers and educators insist on no less than the highest standards concerning the resources that will impact our country's future: our children.

Carolyn T. Roberson,
Sr. Coordinator, Instructional Technology, Norfolk Public Schools

Carrie Gardner

Carrie Gardner is a member of the Board of Directors of the Pennsylvania School Librairans Assocation. She is also a doctoral candidate at the University of Pittsburgh. Her research examines the conflict resolution behaviors used by school board members, principals and school library media specialists during the creation and implementation of Student Internet Use policies. She is also Coordinator, Library Media Services at the Milton Hershey School. Previously she was the high school library media specialist for the Milton Hershey School. Ms. Gardner received her B.S. in Education/Library Science from Millersville University and her M.L.S. from the University of Pittsburgh.

I. Introduction

My name is Carrie Gardner. I am the Coordinator of Library Media Services at the Milton Hershey School in Hershey Pennsylvania and a Ph. D. Candidate at the University of Pittsburgh. The opinions expressed during my testimony are mine alone and do not necessarily represent those of either institution. Thank you for the opportunity to discuss the issues surrounding our children and the Internet.

II. Role of a School Library Media Center

The school library plays a unique role in the education of America's children. It is the one academic unit in the district that serves every student regardless of their course selection or academic ability. There are four main missions of school libraries:

Promote literature and reading.
School libraries provide our young people with quality literature. Exposure to literature promotes the acquisition of reading skills that students must have in order to be successful in school and later life.

Provide information that supports the curriculum.
School libraries provide resources our young people need in order to complete their class assignments. The days of using only a textbook to learn and produce from are gone.

Teach our young people how to find, process and use information.
School librarians provide instruction so students become critical consumers and efficient users of information. Employers and institutions of higher education tell us that our 18 year-olds must know how to use e-mail, mine information from the world wide web, and efficiently use technology to accomplish tasks. School librarians work each school day to help students master these skills so they can lead productive lives during this digital age.

Provide information students need as they grow into adulthood.
Because our young people can not drive, they often can not access the information available at a public library. Because of this, school library media centers contain information about the world we all live in. Young people use this information for all sorts of different tasks: to obtain The Boy

Scout Eagle Award, to become a better athlete, or to discover if what their uncle is doing with them is "normal."

III. Our Young People

School libraries serve America's children. I would like to paint a picture of those children:
1 in 2 will live in a single parent family at some point in childhood.
1 in 3 is born to unmarried parents.
1 in 3 will be poor at some point in their childhood.
1 in 5 is born to a mother who did not graduate from high school.
1 in 5 has a foreign-born mother.
1 in 6 is born to a mother who did not receive prenatal care in the first three months of pregnancy.
1 in 6 has no health insurance.
1 in 8 never graduates from high school.
1 in 12 has a disability.
1 in 24 does not live with either parent.
1 in 4 girls will be sexually abused by the age of 18.
1 in 7 lives with a family member who abuses drugs or alcohol.

Our young people practice a variety of religions and have varied ethnic backgrounds. Thanks to the almost ubiquitous presence of television, radio and the Internet, they know about every hungry child in Africa, shooting, rape, robbery, and murder in their town, state, nation and the world. They start to carry the weight of the world with them at a very early age.

IV. The Intersection of School Libraries, Young People and the Internet

Two benefits of the Internet to our young people include:

The amount of information available. Access to the Internet provides school libraries with an unprecedented opportunity to provide students with a HUGE amount of information from very reliable sources along with a HUGE amount of, shall we say—misinformation, opinions, and advertisements.

The "instant" delivery of information. The vast amount of information on the Internet is accessible within seconds. Having information available at such a quick pace allows teachers, school librarians and students to spend the majority of their time evaluating and using the information, instead of searching for the information.

In order to support the curriculum, middle and high school librarians and the young people they serve face situations such as these every day:
Students in speech class debate capital punishment, needle distribution programs and other social issues in their quest to fine-tune their debating skills. Persuasive speech topics for students as young as 8th grade often include gun control and abortion. Economics students need statistics on HIV/AIDS infection rates in Africa in order to complete assignments on the economic impact of the disease. Health students study how HIV, syphilis, herpes and a host of other diseases are transmitted in hopes that they will take appropriate precautions.

The curriculum taught in every school district includes topics that make adults uncomfortable, but are necessary so our young people are engaged learners and discovering the information they need to understand the issues that will affect their adult lives.

During my time as a building-level school librarian I watched, day in and day out, as students casually browsed the web looking the information they needed. They weeded through countless sites looking for those that provided the information they needed or wanted. Rarely were they sidetracked by a catchy web site. When armed with the skills needed to navigate, understand and use the Internet, they do just fine.

V. Scenarios in Place

School districts have taken a number of different approaches to student Internet access.

Unlimited
Students and adults have no technological restrictions to reaching information on the Internet.

Filtered
Scenarios include those where students can only use a filtered computer but the adults have unfiltered access. Other districts filter all computers. There are a variety of filter products available. Some work by blocking all sites and allowing access to only selected sites. A survey in the November issue of School Library Journal showed that 58.3% of school districts filtered Internet.

Filtered Everywhere but in the Library
Many districts filter everywhere but the library. They recognize that the mission of the school librarian is to teach the young people to handle information.

Parental Permission
Some districts have instituted policies that require parents to sign a permission slip before their young person is allowed on the Internet. Other districts have taken the opposite approach and give every student access unless their parents have signed an "opt-out" form.

Student Acknowledgement Forms
Districts have passed policies that require students to sign a form which states the do's and don't of Internet activities.

Teacher Use Only
Some districts insist that adults be at the keyboard and mouse. Students are not allowed to physically touch an Internet accessible computer.

No Internet Use in the District
A few districts in the country feel that the Internet is such a dangerous place that it should not be in the district. Some have gone so far as to say that no information from the Internet can be used with students.

VI. The Road Less Traveled

The purpose of a K-12 education is to prepare young people to be productive citizens. Employers, colleges, trade schools and common sense tells us that in order for our young people to work in the global economy, tackle the social issues of the day, and have fulfilling lives, they must be able to navigate the Internet. This ability is not genetic or acquired via osmosis.

Children must be taught how to deal with the racism, violence, sexually explicit information, and every other trait, both good and bad our society has to offer both in real life and cyberspace.

It is the road less traveled to teach every child how to use, understand, and at times ignore what they find on the Internet. If we don't equip our youngsters with these skills, we run the risk that they will stumble upon access at a friends house, the church office, the public library, Grandma's house, even the school library; and engage in, at best an inappropriate behavior and at worst, a behavior which causes them physical or emotional harm.

Again, thank you for the opportunity to address this committee.

References

II. Role of the School Library Media Center

Information Power: Building Partnerships for Learning. Association for Educational Communications and Technology and American Library Association Chicago: IL, 1998.

This volume provides standards that if met, provide students with solid background in information retrieval, use and synthesis.

American Association of School Librarians Web Sites:
www.ala.org/aasl/ip_nine.html: Standards for Student Learning

www.ala.org/aasl/positions/ps_roleschool.html: The Role of the School Library Media Program

Krashen, Stephen D. The Power of Reading: Insights from the Research. Libraries Unlimited, Englewood: CO, 1993.

This volume provides references to the benefits of reading.

Haycock, Ken. What works: Research about teaching and learning through the School's Library Resource Center. Rockland Press, Seattle: WA, 1992.

III. Our Young People

The State of America's Children Yearbook 2000
www.childrensdefense.org/keyfacts.html

V. Scenarios in Place

The Commission on Online Child Protection web site lists filter products along with research studies on their use.
Main web site: www.copacommission.com

A University of Pennsylvania study
www.copacommision.com/papers/filter_effect.pdf

Biography Detective Michael Sullivan
Naperville Police Department

Detective Sullivan is a twenty-year veteran of law enforcement and holds a Bachelor's Degree in Law Enforcement Administration from Western Illinois University. During his career he has been involved in every type of criminal investigation at the local, state and federal levels. For six years Detective Sullivan served as a member of State and Federal Narcotic Tasks Forces, working in an undercover capacity. He now brings the techniques learned during his time on those task forces to investigations of crimes committed using the Internet.

Besides his duties at the Naperville Police Department Detective Sullivan is on the teaching faculty at North East Multi-Regional Training, The College of DuPage, The Suburban Law Enforcement Academy and the Federal Law Enforcement Training Center in Glyco Georgia. Detective Sullivan has also been a guest lecturer for Assistant United States Attorneys at the Department Of Justice, Office of Legal Education Training Center in Columbia South Carolina.

As a lead investigator for the Illinois Attorney General's Task Force on Child Pornography and Internet investigation Detective Sullivan's innovative techniques have resulted in the arrest and prosecution of numerous predators of children. Currently he is teaching those techniques to local, state and federal law enforcement officers and prosecutors in the Midwest. He is the creator of the SAFEKIDS program in conjunction with the Microsoft Corporation, which is a course of instruction for children from the 4th to 6th grade on the dangers of the Internet. The program uses a workbook, lecture and a fully narrated slide presentation to give children the skill to deal with predators on the Internet. In the creation of the slide presentation nationally know news reporters from ABC New and Good Morning America loaned their voices to the characters in the presentation. Detective Sullivan has received numerous awards for his work including the Medal of Valor, Meritorious Service Medal, The Illinois Bar Association's Law Enforcement Official of the Year 2000, and the local J Edgar Hoover award from the VFW. His efforts have also been the focus of a story in The Ladies Home Journal, ABC Television News Program 20/20 and on The Oprah Winfrey Show.

Testimony Of Detective Michael Sullivan

With the limited time and resources available to law enforcement today, it is imperative that whatever actions or assistance comes from new laws or guidelines for the Internet, those actions must have the greatest impact in the area that most negatively affects our children. Since nineteen ninety four the Naperville Illinois Police Department's Computer Crimes Unit has been involved in more than five hundred computer crime investigations. The vast majority of those investigations have involved crimes of child exploitation and molestation. The alarming growth in reported crimes involving child exploitation is not specific to Illinois, the Midwest or even the United States. The growth of crime in this area is best shown in the statistics gathered by the Federal Bureau of Investigation's, Operation Innocent Images, where for the past two reporting years they have shown a twelve hundred percent increase in computer related child exploitation crime.

The bulk of the child exploitation takes place in the form of child pornography or sexual solicitation of a child. In the six years that the Naperville Police Department, and the Illinois Attorney Generals' Child Exploitation Task Force have investigated these types of crime, we have found that more than ninety five percent have involved attempted physical contact between the child and the predators. . The most dangerous areas of the Internet for children are chatrooms and one on one messaging ie. Instant Messenger. Most cases we have investigated involve the use of a chatroom and instant messaging system or "whisper" mode. This format allows the offender to search out their victim in a "virtual park", selecting their age, sex and geographical location. After observing the chat conversations of their potential victim the predator checks the profile for background information. This is the basic information needed to approach the child. The next, more serious, approaches are made in an instant message and E-mail format.
On-line child predators come from every walk of life. We have arrested businessmen, managers, ministers, schoolteachers and members of every branch of the military. In one case we had a schoolteacher drive twenty-two hours From Texas to Chicago to molest a high school freshman. In another case a man drove eighteen hours through a blinding snowstorm to get to his 12-year-old male victim. After being apprehended the pedophile admitted to sexually molesting 35 other children. And still in another case the child's parents discovered the online contact with the predator and they terminated the online account. However, the parents did not know that the relationship online had already become sexual in nature. The child, now convinced that the predator was a better friend then her parents, continued the online contact via computers at her school. In this case the predator made arrangements to meet the child at her school. The predator met the child in the school parking lot and molested her on school grounds.
Typically we have seen the following types of behaviors during the luring process:
The predators will build trust by asking the child to perform simple tasks that help the predator confirm that they are speaking with a child such as requesting a telephone call from the child to hear the child's voice. The predators will continue with sexual requests such as; sexually posed images or nude images. The child can use a digital camera or scanner to send photos via e-mail and if they do not have access to these devices they will

send photos via the mail. Unfortunately, a child in search of a friend, will agree to these requests, and are easily coerced into committing sexual acts. Most important they commit acts of deception to prevent parents from finding out about the relationship. Generally, the approach by instant messaging is not observed or documented by parents, ISPs or filtering technology. However sites such as FREEZONE.COM use live adult supervision to monitor chatroom behavior and do report attempted violation of law to the police. Other products monitor chat rooms, and bar the potential predator from the chatroom for flagrant or obvious solicitations, and still other products allow the parent to turn Chat and instant messaging off so it is not available to the child. . However this is not the norm in most on-line services, and the attempted sexual solicitation of the child is never documented or reported. The predator is sent, undocumented back to the chatrooms in another area, to look for another unknowing, and unprotected victim.

To better understand why documenting such actions is vital, you must realize that if you allow your child to go online unprotected, they will see sexually explicit content, they will be spoken to in a profane nature and they will be speaking with sexual predator. That is one hundred percent guaranteed.

Unfortunately, all to often we are called in to assist in the investigation after a child has been molested. We join the local Police Department's investigator at the hospital and try to explain how the child was approached online. Then, what can be done to locate the predator, secure the necessary evidence to arrest and convict the predator. As the facts surrounding the meeting between their child and the predator unfold they find out that this predator has molested other children in other areas of the country, and that his chats, even though were monitored, those attempts were never reported. The activities of the predator were never documented or given to anyone in an attempt to stop the abuse. Instead, the predator was free to continue roaming the Internet searching for other children to molest.

I believe existing technology, properly applied, will prevent an on-line predator from establishing a relationship with a child. The predator can be stopped months before a "real world" meeting could be arranged.

I know from my work that there are several very important issues concerning blocking, filtering or censoring any content on the Internet. But looking beyond that, the issue of child exploitation especially regarding child predators should have the highest priority. Software to enable parents and educators must be one based on content and not address blocking and must be able to scan all facets of a child's computer activity. This especially includes chat, whisper modes, browsers, e-mail and attachments. Content that is sexually explicit, harassing, predatory or even death threats can be filtered and kept away from children.

We have found two products that can monitor in all of these areas and provide law enforcement with sufficient information to take further action against an on-line predator. They are Cyber Sentinel and Predator Guard. The anti-predator libraries included in these products were developed in conjunction with multiple on-line predator investigations and are very effective. Predator Guard is interesting because it can be used on top of any other filtering solution. It is used strictly for the detection of Child Predators and provides an important layer of protection. The most critical part of this software is that it takes a screen capture of the prohibited material and stores it in a secured database, that only the parents have access to. They can view the violation, and determine if law enforcement needs to be informed and then discuss the violation with their child. Parents are able to supervise their children's on-line activities without standing over the computer. I believe the most successful way to help protect our children is to empower parents with awareness and simple, effective software that allows the parents to detect a problem **before** it reaches my desk.

Thank You for the opportunity

Lawrence Lessig
Professor of Law, Stanford Law School

Lawrence Lessig is a Professor of Law at the Stanford Law School. He was the Berkman Professor of Law at Harvard Law School. From 1991 to 1997, he was a professor at the University of Chicago Law School. He graduated from Yale Law School in 1989, and then clerked for Judge Richard Posner of the 7th Circuit Court of Appeals, and Justice Antonin Scalia on the Supreme Court. Lessig teaches and writes in the areas of constitutional law, contracts, comparative constitutional law, and the law of cyberspace. His book, Code, and Other Laws of Cyberspace, is published by Basic Books. In 1999-2000, he was a fellow at the Wissenschaftskolleg zu Berlin.

MEMORANDUM

06 August 2000

TO: COPA Commission
FROM: Lawrence Lessig
RE: Proposed legislation to zone minors from material deemed harmful to minors

As you have requested, I have summarized my views about the trade-offs among various proposals for zoning minors from material deemed harmful to minors in cyberspace. I have drawn this analysis from my article with Paul Resnick, Zoning Internet Speech, 98 Michigan Law Review 395(1999). Any analysis of the constitutional issues raised by these proposals can be found in that article. My aim in this memorandum is simply to outline the alternatives, and the trade-offs among them.

As I said in my testimony, in my view your objective should be to identify techniques to enable parents to protect children, consistent with protecting the values of free speech. In my view, however, free speech is threatened both by bad law, and by bad code. My aim has been to identify a response that minimizes the effect of bad code. I offer Proposal (4) as an example.

INTRODUCTION

To zone minors from material considered "harmful to minors," a system must know the (1) age of the recipient and (2) the content of material the recipient wants to view. If the recipient is a minor, and the content is harmful to minors, then the system should block access; if the recipient is not a minor, or the content is not harmful to minors, then the system should not block access.

To facilitate such zoning, proposals to date have been of two general sorts. First, there have been legislative proposals to require that adults carry identification when they desire to get access to material that is harmful to minors.[1] (I will refer to proposals of this sort as Proposal (1).) Second, there have been nonlegislative proposals to facilitate the rating and filtering of content on the Internet, thereby enabling parents to block access by their children to material that is harmful to minors. ("Proposal (2)").

---

[1] The first federal proposal required identification whenever the adult sought access to "indecent" material, but the constitutional standard has only ever justified conditioning access based on whether material is "harmful to minors."

Proposals of the first sort have not been successful in federal courts. The burden on adults to carry age-identification is significant; the burden on sites to verify the identification presented is also high. These two burdens have been considered too great in light of less burdensome alternatives. Every federal court to review these statutes has concluded they are unconstitutional.

Proposals of the second sort have also been met with great skepticism, though this skepticism is of more recent origin. Technologies for rating and filtering content on the Internet are inherently flawed. They universally reach beyond the narrow category of harmful to minors material. They therefore facilitate a far greater blocking of access to material than the government's legitimate interests reach. And while this blocking is done by individuals, and not governments, the effect of these proposals on access to controversial speech, even by minors, should be relevant in evaluating the merits of these proposals.

The solutions, in my view, are either proposals that (3) facilitate a less burdensome kind of identification, or proposals that (4) induce a less extensive form of rating and filtering. Proposals of type (3) depend upon systems that certify that the user is a minor, not that the user is an adult. And proposals of type (4) identify simply whether content is harmful to minors, and not anything more.

In the analysis that follows, I first describe proposals (3) and (4). Within each description, I identify the strengths and weaknesses of each proposal. I then describe how each proposal is complicated if the "harmful to minors" standard is different within different geographic communities.

PROPOSAL (3): IDENTIFYING MINORS

Imagine a browser that gave users the option to establish a "profile" that governed the preferences of the browser for that user.[2] That profile would be protected by a password, so that when the user "logged onto" the browser, he or she would have to supply a password. Once the identity of the user is verified, the browser would then select the bookmarks, and user preferences desired.

Imagine further that in setting up the user profile, there was an option to designate that the user was a minor. If that option were selected, then the browser would not permit the transmission of personal data to a web site.[3] It would also, if requested, certify to a web site that the user was a minor.

Finally, imagine that a law required web sites serving material deemed "harmful to minors" first verify whether the user was a minor by "querying" the user's browser about whether the user was a minor or not. That query would simply be a request to the browser that it transmit whether the profile of the user was marked as a minor; the browser would answer in the affirmative if it was so marked. If the client answered affirmatively, then this law would forbid the server from serving that material to the minor. If the client did not answer affirmatively, then the server would be free to serve the material without legal liability.

This configuration of technological capacity and legal responsibility would facilitate, to some degree, the zoning of minors from material deemed harmful to minors. Browsers are essentially free. The modifications required to facilitate the identification of minors would be trivial. And the software to enable servers to query and block sites based on that code would be relatively easy to implement as well.

Nonetheless, Proposal (3) would impose burdens on Internet speech. In the balance of this section, I describe these burdens. I then describe the legislation that would be needed to move the net in the direction of this configuration. That legislation is what I will describe as Proposal (3).

---

[2] While I have abstracted this description from the particulars of any specific existing technology, it is clear that there are many existing technologies that come close to the description I offer here. The Netscape browser permits different user profiles. The Mac OS 9 permits profiles specified at the operating system level. There is no reason these technologies could not be made more generally available.

[3] This is a complicated objective. Certainly it would be easy to ensure the browser itself does not send any of the personal data stored in its preference files. But it would be harder to interpret a web page to determine whether an email address or other personal information was being requested.

The Burdens

The burdens of this configuration are two: first, the burden on any site to determine whether its content was "harmful to minors." Second, the risk of misuse of the identifying information that the user of a particular browser is a minor.

The burden of rating material "harmful to minors"

The first burden is no greater than exists under real space laws that restrict access to material harmful to minors, except to the extent geography becomes relevant. (I will discuss this qualification below). Sites offering material that is harmful to minors today must take steps in many states to identify that material, and keep it from children.

Nor is the burden any greater than exists under Proposals of type (1). They too require the site to determine whether it must block access based on age; that determination requires the same sort of judgment required by Proposal (3).

Moreover, relative to a world dominated by systems following Proposal (2), the effective burden of Proposal (3) on sites may be less. The risk with Proposal (2) is that third party ratings may mistakenly block sites. At least the owner of the site has control over whether the blocking occurs in a world with Proposal (3).

Nonetheless, except for the possible benefit of more accurate rating, forcing sites to identify whether their content is "harmful to minors" is a burden relevant to considering the constitutionality, and advisability, of such a proposal. [4]

The risk of misuse of the "minor" certificate

The more significant criticism of Proposal (3), however, is the risk that a signal that a user is a minor would increase the risk that minors will suffer from illegal behavior.[5] Depending upon how the signal was constructed, it could be a simple matter for someone seeking children on the Internet to induce the client to identify that the user was a child. That information could then be used to facilitate abuse.

---

[4] Note that the burden of requiring labeling is not quite as significant as it is in real space. To an ordinary user viewing the site without a "kids-enabled" browser, the label would be invisible. The only people who know how the site is labeled are those that have enabled discrimination based on the label.

This risk could be minimized. For example, browsers could be coded to reveal the age of a user only to servers that have been certified to request that information. This would cut down on the improper querying of age information. Second, because it would be easier for law enforcement to identify users who are improperly querying the age identifier, Proposal (3) might well facilitate a better system for tracking down those who would abuse children.[6]

Nonetheless, this risk is a reason to be skeptical of Proposal (3), and to prefer another that might achieve the same benefits without this particular risk. This, in my view, is just what Proposal (4) would do.

The Necessary Legislation

The legislation necessary to realize the configuration I have described is relatively simple.[7] In my view, it would require two parts. First, it would direct a regulatory agency (which I will assume is the FCC) to specify, in consultation with Internet standards bodies, (a) a minimal protocol to query a client about whether the user was a minor, and (b) a standard for answering such a query. Second, it would direct any server with a substantial custom coming from the United States to implement the protocol for querying and blocking based on age if that site is serving material that is "harmful to minors."

---

[5] Some have argued that Proposal (3) is no different from Proposal (1), since in both cases age must be certified, and the costs of certifying would be the same under both proposals. This is a mistake. Under Proposal (1), age must be certified by some third party, because holding an adult ID gives users access to information to which they otherwise might be blocked from gaining access. There is an incentive, therefore, to lie in securing an adult ID. But a minor-ID would not create any incentive to lie. Indeed, there would be no reason not to allow people to lie about whether they were a minor. Anyone who would want to assure that they were not exposed to material deemed harmful to minors could simply so indicate. Since there is no reason to be certain that a person is truthfully indicating, there would be no need for a third party certification.

[6] Law enforcement, for example, could flood the net with clients pretending to be children, so increasing the odds that an offender would be identified that it would make the net a very dangerous place for child sex-offenders.

[7] All of the legislation that I will describe is civil regulation. In my view, there should not be, and possibly cannot be, criminal regulation in this context. It would be sufficient to impose civil fines on sites that violate the rules proposed here. At least Congress should begin with that assumption, and increase the penalties only upon a showing that sites are not generally complying.

In my view, no legislation would be required to induce compliance on the client side. If there were a simple protocol to query and block based on age, and if sites were required to implement this protocol, then software providers would have a significant incentive to develop tools to implement this protocol and enable parental choice. The legislation, in other words, would create a market that software providers would have an adequate incentive to serve. There would therefore be no need to regulate either the makers of browsers, or the suppliers of operating systems for computers. That part of Proposal (3) would, in a sense, take care of itself.

PROPOSAL (4): THE HARMFUL TO MINORS LABEL

Proposal (4) differs from Proposal (3) in one small, but significant, way. Under both Proposal (3) and (4), sites carrying material harmful to minors would have to rate that material. But while under Proposal (3), the site would block access if the client indicated the user was a minor, under Proposal (4), it is the client that blocks access if the site signals that it is serving material harmful to minors. The critical difference then is that the client does not reveal that the user is a minor; therefore the risks of that revelation are avoided.

This proposal imagines the following configuration:

First, that there was a simple protocol for sites to signal that they were carrying material deemed harmful to minors.

Second, that web browsers were configured as described above, to facilitate different password protected user profiles, as well as the ability to mark that the user of a particular profile was a minor.

Third, that when a client browser using a profile that indicates the user is a minor comes across a site that signals that it is carrying material harmful to minors, the browser blocks access to that site.

With this configuration of technology, parents who wanted to protect their kids from access to material harmful to minors could do so by using a browser so configured – assuming, of course, that suppliers of material harmful to minors displayed a common label indicating as much. Proposal (4) would induce that display, by mandating that servers with material harmful to minors indicate that fact by adopting a common, or specified, label.

In the balance of this section, I consider the benefits and costs of this proposal.

Burdens

The burdens of this configuration of technology and legal requirements are, in my view, the least among the four proposals. Like proposals (1) and (3), this proposal would require sites to label their content. But again, as with Proposal (3), this self-labeling would reduce the risk of mislabeling by third parties. Thus while this requirement would no doubt be a burden on sites carrying material deemed harmful to minors, it would not be a burden that was disproportionate to other proposals, or to the burden on providing such content in real space.

This proposal too would require modification of browser code to enable minor-marked profiles and the blocking of sites that identify themselves as carrying material harmful to minors. But again, both changes in code would be trivial. And if sites generally complied with a requirement to label harmful to minor material, then the market would create a significant incentive for suppliers of browsers or operating systems to facilitate such blocking. Thus legislation effecting this requirement would create a market for software authors to develop child protective software.

Legislation Required to Effect Proposal (4)

The legislation required to bring Proposal (4) into effect is simpler than the legislation necessary to bring into effect Proposal (3). The legislation would direct both an agency and web sites. But the task of both would be simpler under Proposal (4) than under Proposal (3).

Direction to the FCC

Under Proposal (4), an agency would, in consultation with Internet standards bodies, determine a label that a web site could transmit when initiating contact with a client to signal that content on a particular page was harmful to minors. This protocol could in principle be a simple label, <htm>, </htm>. But how best to implement this would be a judgment initially made by Internet standards bodies.

Direction to web sites

Web sites that carried material harmful to minors would then be required to signal that fact upon connection with a client. The web site would not be required to implement any logic for dealing with the client (as in Proposal (3)). Like a label that indicated that food contained sugar, thereby enabling a diabetic to properly respond, this label would simply signal to a user the fact that the site has judged the material on that page to be harmful to minors. And again, as this label would be buried in the code of a web page, the user would not realize a site is so labeled unless his or her browser was enabled for minor-rated browsing.

Results

If web sites complied with this requirement, then a significant market would develop to take advantage of this additional information being provided by servers. Suppliers of browsers or operating systems would market updates to their technologies so that parents would be able to take advantage of this information. Schools as well could use this information to restrict access on the Internet for computers within their control. No regulation of browser or operating system manufacturers would therefore be required. As with Proposal (3), the market, in a sense, would solve this part of the proposal itself.

The Proposal Compared

Proposal (4) is preferable to, in my view, each of the other three proposals, and to doing nothing at all. In the balance of this section, I sketch reasons why.

Advantages over Proposal (1)

Like Proposal (1), Proposal (4) depends upon a form of identification — that the user is a minor. But unlike Proposal (1), there is no need under Proposal (4) for users to secure costly third party identification. Nor, for the reasons I described above, is there any need for web sites to engage in costly verification of the identification. The assertion made under Proposal (4) (that the user is a minor) is not a claim that anyone has a reason falsely to assert, or if they do, no one has a reason to correct that falsity. Proposal (4) is better than (1), then, in that it reduces the cost of identification.

Advantages over Proposal (2)

Like Proposal (2), Proposal (4) makes the choice to block content an individual's. No site is required, under this proposal, to block content on its own. But unlike Proposal (2), Proposal (4) would not necessarily lead to labels or filters beyond the narrow class that the government has a legitimate interest in regulating. Individuals may still desire a more comprehensive set of tools for restricting access to Internet content. But the absence of an effective minimum would not artificially increase the demand for more extensive measures.

Advantages over Proposal (3)

Like Proposal (1) and (3), Proposal (4) depends upon a form of identification. Like Proposal (3), it depends upon a form of identifying that the user is a minor. But unlike Proposal (3), that information is not made available to others on the network. The fact that a user is a minor affects just what his or her browser does; it does not signal that fact to other sites. Thus the proposal would not create the risk of abuse for children using the net, though it would, if properly implemented, increase the protection for children.

Advantages over doing nothing

Thus, in my view Proposal (4) trumps each of the three other proposals for zoning minors from material harmful to minors on the Internet. So too does it, in my view, trump the proposal of doing nothing. The consequence of doing nothing is to increase the demand for products based on Proposal (2). As organizations such as the ACLU, and Peacefire, have made abundantly clear, these technologies have imposed a significant cost on free speech on the Internet. The demand for such products would be limited, in my view, if a viable and less restrictive alternative were available. That provides an affirmative reason to prefer regulation over doing nothing.

THE COMPLICATION OF GEOGRAPHY

The one complicating factor in the whole of this analysis is the effect of community standards upon any solution. In principle, it is possible that what is "harmful to minors" in one area of the country is not "harmful to minors" in another. This is possible, at least, though it is by no means necessary. Movies rated "R" or "X" are not rated differently depending upon the part of the country in which they are being played. It is not clear why Internet content would have to be any different.

This is an uncertain issue jurisprudentially, simply because the case that ratified the "harmful to minors" standard, *Ginsberg v. New York*, 390 U.S. 629 (1968), described such material as "obscenity for children." The case was decided, however, before the modern standard for determining obscenity was finally settled upon. Thus it is unclear to what extent the "harmful to minor" standard must be adjusted to different communities. If, as the Third Circuit recently indicated, it does, then this would increase the complexity for all four proposals.

Proposal (4) could incorporate a geographically based difference, though it would raise the costs of the proposal significantly. Rather than simply providing a harmful to minors label, the label would have to indicate harmful to minors in X, where X was a geographic location. That would then set a standard that the client would have to judge relative to. If the jurisdiction of the child were more conservative than site X, then the fact that something was harmful to minor in X would entail it was harmful to minors in the client's jurisdiction. The contrary, however, would not necessarily follow.

The Supreme Court has not finally resolved this question of geography. If they resolve the question in favor of community standards, then this may make *any* regulation too cumbersome. For the reasons I have offered in favor of some regulation over none, in my view, that would be unfortunate.

CONCLUSION

The aim of policy making in cyberspace must be to consider the interaction between law and technology, and to recommend regulation only for that part of a policy problem that will not take care of itself. My aim in this analysis has been to suggest the least invasive form of regulation that will avoid the apparent consequence of no regulation – the spread of "censorware" technologies, or Proposal (2) technologies. Proposal (2) technologies are, in my view, as harmful to free speech values as bad law could be. My aim has been to identify good law that might avoid this bad code.

PEOPLE
FOR THE
AMERICAN
WAY
FOUNDATION

Elliot M. Mincberg

Elliot Mincberg is vice president, general counsel and legal and education policy director of People For the American Way Foundation, a 300,000-member national organization that promotes public education and constitutional and civil rights. He has served as co-counsel in a number of important First Amendment and education cases, including litigation successfully challenging the Communications Decency Act and a mandatory public library Internet filtering policy. He serves on the board of directors of the Internet Education Foundation and has written and spoken extensively on First Amendment issues. Prior to joining PFAWF, Mincberg was partner at the Washington law firm of Hogan and Hartson, where he specialized in education and civil litigation. He received his law degree with honors from Harvard University in 1977 and his undergraduate degree with honors from Northwestern University in 1974.

BEST COPY AVAILABLE

2000 M Street, NW ♦ Suite 400 ♦ Washington, DC 20036
Telephone 202.467.4999 ♦ Fax 202.293.2672 ♦ E-mail pfaw@pfaw.org ♦ Web site http://www.pfaw.org

PEOPLE
FOR THE
AMERICAN
WAY
FOUNDATION

Written Testimony of Elliot Mincberg of People For the American Way Foundation For the Commission on Child Online Protection On "Policy Implications of Filtering, Labeling and Rating"

July 21, 2000

On behalf of the more than 300,000 members of People For the American Way Foundation ("People For") across the country, I would like to thank the Commission for the invitation to testify on this important subject. When it comes to the Internet, tools and techniques like filtering and rating are neither inherently good nor inherently bad. Instead, the question is how are filtering and labeling used. In particular, how can they be used to promote what we regard as the key objective of empowering families and other internet users to decide for themselves what to see and do on the Internet? To People For and its members, that is the central question to answer concerning the policy implications of filtering, labeling, and rating on the Internet.

Founded in 1980 by a group of civic and religious leaders, People For is a national civil liberties and civil rights organization that is dedicated to promoting and defending fundamental American values and freedoms, including freedom of speech, public access to valuable information, educational opportunity, diversity, respect, and tolerance. We have been deeply involved with issues concerning the Internet, particularly as they relate to public libraries and families. With respect to litigation, People For served as co-counsel and co-plaintiff in the Reno v. ACLU lawsuit which resulted in the Supreme Court unanimously striking down the Communications Decency Act in its most significant respects. We are currently helping to represent a group of Internet companies such as PSINet, Inc., nonprofit organizations, and citizens in a challenge to a Virginia law restricting the Internet similar to

2000 M Street, NW ◆ Suite 400 ◆ Washington, DC 20036
Telephone 202.467.4999 ◆ Fax 202.293.2672 ◆ E-mail pfaw@pfaw.org ◆ Web site http://www.pfaw.org

the prohibitory aspects of COPA, PSINet Inc. v. Chapman. We have participated as amicus curiae in significant Internet-related litigation. This has included the lawsuit in which the Third Circuit recently struck down the prohibitory aspects of COPA itself, and the California case of Kathleen R. v. City of Livermore, in which we have supported the city's position that public libraries cannot be held liable for material that the library does not publish but simply carries by providing Internet access to library patrons. Finally, we helped represent an outstanding civic organization called Mainstream Loudoun, as well as individual parents and residents of Loudoun County, Virginia, in challenging one of the most restrictive public library Internet policies in the nation in Mainstream Loudoun v. Board of Trustees of the Loudoun County Public Library. In that case, the federal court issued a thorough 46-page opinion granting summary judgment against Loudoun County's mandatory Internet filtering policy as unconstitutional under the First Amendment of the Constitution.

We have also been significantly involved in developing policies and practices concerning the Internet. We have worked with industry representatives and many others in helping develop and promote GetNetWise, the Internet site and strategy that helps inform parents and all Internet users about filtering and many other methods to help users more effectively control their use of the Internet. We have worked with parents, citizens groups, libraries, and others in communities across the country to help deal with Internet access issues. I serve on the boards of the Internet Education Foundation and the Center for Democracy and Technology. We participated in several White House Internet summits that focused in large part on the issues of kids on-line as well as parental and user empowerment. We have also testified on such issues before the National Commission on Libraries and Information Science, the U.S. Senate Committee on Commerce, Science, and Transportation, and the National Research Council. A copy of my Senate testimony, which is particularly relevant to the issue being considered today, is enclosed with this testimony.

The Promise of the Internet and the Use of Filtering and Rating

As an overall perspective, the promise of the Internet particularly for young people and future generations is tremendous. The Internet is the communications medium of the 21st century and provides unprecedented opportunities for education, personal growth, and career development for current and future generations of Americans. Indeed, being computer and Internet literate has become an essential skill for children growing up today. There is no question that among the vast materials available on the Internet is some false, misleading, sexually explicit, and hateful content. However, as the Supreme Court found in striking down the Communications Decency Act, there are significant differences between the Internet and broadcast media, including the fact that users affirmatively decide what information to see on the Internet. The issue that this Commission faces is how to handle the existence of such information on the Internet within a legal and policy framework that maximizes the benefits of the Internet, and respects the rights of families and other Internet users to decide what to read and do on the Internet consistent with individual and family values and circumstances.

Tools like filtering can play an important role in helping resolve such questions. Unlike prohibitory legislation like CDA or COPA, filtering allows decisions on Internet use to be made at the user end. That means that parents can limit or control what their own children see and do on the Internet without restricting everyone on the Internet to only what is fit for children. With a wide variety of filtering and other products, categories, and levels, families can adapt filtering or other techniques to their own interests and needs. Unlike legislation like CDA, which cannot affect content overseas, filtering can control access to all Internet content, whatever its source.

On the other hand, filtering and labeling also have limitations and potential dangers. Decisions about how to filter or label Internet content are generally made by people like software engineers or content providers, not judges and juries. That means that we can never rely on filtering to magically block content that meets legal criteria like "harmful to minors." As we found in the Loudoun county case, even the best blocking or filtering software will block some sites that it should not block and fail to block sites that it arguably should. For example, the filtering software in that case blocked substantial amounts of valuable and clearly non-pornographic information, including websites for the Quaker Society of Friends, the American Association of University Women, the Heritage Foundation, and a site for beanie babies as well as many sex education and gay and lesbian sites. The library staff's own testing of the software from the perspective of a library patron found that more than 65% of blocked sites should not even have been blocked under the Library Board's own policy. Even at the same time that valuable material was blocked, the software did not block substantial amounts of sexually explicit material that arguably should have been blocked under the Library Board's own policy. In addition, there are special challenges with respect to the use of filtering and rating for chat rooms, news groups, and other aspects of the Internet.

Specific Policy Prescriptions on Internet Filtering and Rating

In light of this background, when considering the use of filtering, labeling, and rating on the Internet, five policy principles are particularly important:

First, it is critical that filtering, rating, and labeling systems and software be fully transparent and accessible to the user. Such systems are inherently subjective and variable. To accomplish the most important objective of putting real power in the hands of the Internet user, the user must know precisely what the system does and does not do. That means that systems should fully disclose their criteria and methods for rating or blocking. Filtering or blocking systems with lists of blocked sites should disclose those lists to users. Products should provide maximum user control. For example, individual families should be able to adjust the use of such systems to account for the varying maturity level of minors and to reflect their own values. It will be largely up to the Internet industry to accomplish these objectives. We think there is clearly a role for "Consumer Reports"-type organizations to inform and assist consumers in this area by, for example, grading or rating different filtering and rating systems according to how transparent and user-friendly they are.

Second, government should not mandate the use of filtering, rating or blocking, whether by content providers or by individual families or in institutions like public libraries. The fundamental problem with the Loudoun County policy struck down by the court was that it mandated a "one size fits all" situation, with blocking software required on all computers at all times for all patrons, even adults. Our clients in that case supported an optional filtering policy in which adults and parents would decide for themselves and their children whether to use blocking software, taking into account their own values and needs as well as the flaws and limitations of the software. After the lawsuit, the Loudoun County library adopted just such an optional policy, and all reports indicate that it has been very successful. Other libraries and schools, including a number of Catholic schools, have adopted "acceptable use" policies instead of mandatory blocking and filtering. In addition to the First Amendment problems identified by the court in Mainstream Loudoun, government-mandated use of filtering or blocking frustrates the goal of empowering families and other users to decide for themselves what to do and see on the Internet.

Third, industry should make transparent filtering and ratings systems available, but should not coerce their use. This issue has been raised, for example, with respect to the RSAC/ICRA rating system which, as of January, included self-ratings for some 100,000 Internet sites. Many would oppose systems at the ISP level that would, for example, automatically block any site that did not have an RSAC/ICRA rating. If widely used, such systems would coerce self-rating, even though for many speakers on the Internet, such self-rating remains burdensome, unwieldy, costly, and inappropriate. Examples include the many sites that provide news and art over the Internet.

Fourth, government can play a valuable role in helping encourage and fund ways to improve filtering and other user empowerment techniques, make them more transparent, and make them more widely available and understood. The government's encouragement of what has become the "GetNetWise" project is a good example. In this regard, it is important to keep in mind that there are other user empowerment techniques besides filtering and rating that should be further developed and promoted. These include, for example, technology that allows parents to monitor which web sites their children visit, "contracts" on acceptable Internet use, and methods to guide kids towards Internet "green spaces" with suggested kid-friendly content.

Finally, promoting the effective use of user empowerment techniques is much more effective than attempts at mandatory government control of Internet content such as CDA and COPA. When government seeks to criminalize or regulate speech content on the Internet beyond categories like child pornography, which are illegal for everyone, the First Amendment inevitably gets in the way. So far, every federal or state law like CDA or COPA has been struck down by the courts, by conservative as well as by moderate judges. As discussed above, moreover, promoting control over the Internet at the user end will also be more effective in the long run. While there are challenging policy issues in this area, we encourage the Commission to continue to explore those issues and to seek to find effective ways that will encourage the use of filtering and other techniques so that parents and other Internet users can make the decisions about what to see and do on the Internet.

Thank you very much for the opportunity to testify today.

CRYSTAL ROBERTS, J.D.
LEGAL POLICY ANALYST

Crystal Roberts joined the Family Research Council in the summer of 1997. As Legal Policy Analyst she monitors current trends and developments in Constitutional Law. Her objective is to monitor legal developments affecting families and promote pro-family legal policy by authoring *amicus curiae* briefs, opinion pieces, and articles addressing religious liberty, parental rights, pornography laws, and judicial activism.

Ms. Roberts participates in debates and educational seminars addressing religious liberty and Internet pornography, and has testified in support of parental rights legislation in front of state legislators. While at the Family Research Council, Ms. Roberts has participated in the drafting of *amicus curiae* briefs addressing parental rights, government administered domestic partner benefits, and the application of pornography laws to the Internet.

Ms. Roberts is a 1997 graduate of The College of William and Mary's Marshall-Wythe School of Law in Williamsburg, Virginia and a 1994 graduate of Denison University in Granville, Ohio where she studied history and political science. Prior to joining the Family Research Council, Ms. Roberts clerked for the Free Congress Foundation's Center for Law and Democracy in Washington, D.C., and the public policy law firm of The Rutherford Institute in Charlottesville, Virginia. Ms. Roberts is a native of St. Louis, Missouri.

THE FIRST AMENDMENT IMPLICATIONS OF REQUIRING BLOCKING AND BLOCKING TECHNOLOGY ON PUBLICLY ACCESSIBLE COMPUTERS

Commission on Online Child Protection (COPA)
July 21, 2000
Testimony of Crystal Roberts, J.D.
Legal Policy Analyst
Family Research Council

Mr. Chairman and Members of the Commission. Before I begin my remarks I would like to thank you for the opportunity to address you this morning. The safety of children is of paramount importance to the Family Research Council (FRC). As the Internet has grown and evolved into the important communication tool it has now become, FRC has become increasingly concerned with the astounding ease with which minors have been able to access pornographic material via this revolutionary medium.

Today I'd like to address both the constitutionality and effectiveness of using blocking technology to restrict access to illegal pornography by minors via Internet accessible computers in public libraries. Because a public library maintains complete discretion over the materials that it selects for inclusion into its collection, a public library's act of acquiring intellectual content, whether that acquisition is facilitated through the Internet or one of the traditional means of acquiring material, does not create any sort of public forum with regard to the content included in its collection. Rather, it has maintained a non-public forum. As a non-public forum, a library may restrict material solely based upon its content unless the restriction is unreasonable or constitutes viewpoint discrimination. Furthermore, it is my opinion that even if a judge were to find that, in the absence of an express provision to the contrary, a library had created a limited public forum with regard to the content included in its collection, there are significant compelling interests justifying the use of blocking technology to prevent all patrons from accessing obscenity and child pornography and to prevent minors from accessing material harmful to minors.

Imagine a ten-year-old walking into a public library and requesting a hard-core pornographic video such as "Debbie Does Dallas" or "Deep Throat." Although libraries commonly stock numerous videocassettes, the library will not comply with this request because it simply will not carry such titles. To illustrate, yesterday, I tried to obtain copies of these videocassettes from the Richmond Public Library. As I expected, not only did the library not include these videos in its collection but the librarian also refused to submit my interlibrary loan request for these tapes. Perhaps her reluctance was due to the fact that none of the other libraries from which the library regularly loans books listed the titles in their catalogues either. Just to make sure that the library's inability to meet our request was not merely the result of a more exclusive selection criteria for videotapes, I also asked if they subscribed to *Playboy*, *Penthouse*, or *Hustler*. As I expected, the library did not subscribe to any of these titles nor would it submit an interlibrary loan request to any other regional libraries. As with the videotapes, the other libraries did not list these titles among their magazine collections either.

Now if Richmond's public library has chosen not to provide these tapes, it certainly does not follow that it *must* allow its patrons to access equally graphic images on Internet accessible computers simply because the library has chosen to provide Internet access. Similarly, if the library has chosen not subscribe to *Hustler* in hard copy (a subscription likely to cost approximately $200 annually) it would be terribly inconsistent to argue that the discretionary factors leading to its refusal to select such magazines and videotapes in the first place has suddenly disappeared simply because a patron is using the Internet to facilitate the acquisition of such material. It's just as inconsistent to conclude that the very material that others may be prosecuted for distributing, such as material created in violation of federal copyright laws, obscenity, and child pornography, *must* be provided to library patrons via Internet accessible computers simply because the library provides patrons Internet access. I would submit that such a conclusion is illogical and defies common sense.

Everyday, librarians make choices about what content to select for their collections. There are many factors librarians consider when making this choice — does a particular selection fit the needs of their patrons? Does the selection aid in presenting a wide breadth of knowledge and viewpoints on a particular topic? Finally, does the selection fit with the mission and purpose of the library? In making these choices it is clear that libraries reserve complete discretion to select all material that will be included in its collection. For those of you who don't believe this try walking into a public library and placing your own book on its shelves or, in the alternative, donate a book to your local public library. Rather than immediately accepting your donation, the library is likely to go through the same selection process it engages in when it decides whether to acquire any other book.

The Constitutionality of Blocking Access to Obscenity, Child Pornography, and Material Harmful to Minors Has Yet to Be Fully Addressed By a Court of Law

Despite the public's confusion about the constitutionality of the use of blocking technology in libraries, the current case law is quite clear. No court has held the use of filters to be *per se* unconstitutional. There has been only one case in which a court has addressed the manner in which a public library has used blocking technology. In that case, *Mainstream Loudoun v. Board of Trustees of the Loudoun County Library*, 24 F. Supp. 2d

552 (E.D. Va. 1998), a federal district court held unconstitutional a public library board policy mandating the use of blocking technology to prevent its Internet accessible computers from being used to access material harmful to minors. The court, however, upheld the library board's right to restrict access to obscenity and child pornography on all of its Internet accessible computers. Furthermore, it did not rule on the question of whether the library could install filters on Internet accessible computers located in the library's children's section in order to block out obscenity, child pornography, and material harmful to minors. Therefore, we should not feel the need to limit our consideration of Internet blocking technology when considering the policies that have been proposed to the Commission thus far.

Public Libraries Have Wide Discretion to Regulate the Provision of Internet Access

The constitutionality of a library's decision to select content for inclusion into its collection is based upon a determination of whether the library has created a traditional public forum, a public forum created by government designation, or a nonpublic forum.[1] The forum analysis is the mechanism by which courts assess the extent to which the Government may limit a speaker's access to government-controlled property. Government controlled property is a "traditional public forum" if, similar to streets and parks, it has "immemorially been held in trust for the use of the public and, time out of mind, have been used for purposes of assembly, communication thoughts between citizens, and discussion public questions."[2] A court will conclude that government controlled property is a public forum if "the objective characteristics of the property, such as whether, 'by long tradition or by government fiat,' the property has been 'devoted to assembly and debate.'"[3] Speakers may be excluded from a traditional public forum based upon the content of their speech if that content is not entitled to protection under the First Amendment or when that exclusion is necessary to serve a compelling state interest and the exclusion is narrowly drawn to achieve that interest.[4] The government may regulate the time, place, and manner of expressive activity in a content-neutral manner if the regulation is narrowly tailored to serve a significant government interest and leave open ample channels of communication.[5]

---

[1] *Cornelius v. NAACP Legal Defense & Ed. Fund, Inc.*, 473 U.S. 788, 802, (1985).

[2] *Perry Education Association v. Perry Local Educators' Association*, 460 U.S. 37, 45 (1983) *quoting Hague v. Committee for Industrial Organization*, 307 U.S. 496 (1939) (Roberts, J., concurring, joined by Black, J.).

Under certain circumstances the government may create a public forum in government property that has not traditionally been devoted to broad public use. This "limited public forum" is created when the government intentionally opens "a nontraditional public forum for public discourse.[6] The government creates a limited public forum if "the policy and practice of the government" indicates an intent to "designate a place not traditionally open to assembly and debate as a public forum. … If the government excludes a speaker who falls within the class to which a designated public forum is made generally available, its action is subject to strict scrutiny."[7]

All other property subject to government control can be characterized as either a nonpublic forum or not a forum at all. In a non-public forum government can restrict speaker access if the regulation is reasonable "and not an effort to suppress expression merely because public officials oppose the speaker's view.'[8]

---

[3] *Arkansas Education Television Commission v. Forbes*, 523 U.S. 666, 677 (1998).
[4] *Perry* at 45.
[5] *Id.*
[6] *Arkansas* at 678.
[7] *Id.*
[8] *Perry* at 46.

It is at this point that the *Loudoun County* court made a fundamental mistake. Declaring Loudoun County Virginia's Internet blocking policy a violation of the First Amendment, the court failed to recognize that libraries perform a number of tasks – the performance of each creating legally distinct forums.

After reviewing the county's resolution authorizing the creation of the library, the court ruled that the library board created *a* limited public forum with regard to *all* of the library's function because its "primary objective" of "offering the 'widest possible diversity of views' in many different media," indicated the county's intent to create a "public forum for the limited purposes of the expressive activities they provide, including the receipt and communication of information through the Internet."[9]

Certainly, when libraries determine which patrons may be admitted to the library, they have created a limited public forum for the purpose of determining the activities those on the premises may take part in. However, there is a legal and practical difference between the services the library offers when it invites the public onto its premises for the purpose of accessing the publications in its collection and when the library selects intellectual content. Quite simply, the main task of a library is to select materials and all libraries are selective about their content – much more so than they are about whom enters their premises. To reject this premise is to assert that by stepping onto a library's premises an individual is granted a constitutional right to place a book of their choice on its shelves. Certainly, no librarian would concede that much freedom to those individuals he or she would welcome into the library to enjoy its resources.

The *Loudoun County* court's failure to make this distinction is indicated by the fact that it used as precedent a case involving the removal of a homeless man from the premises of a library which in no way implicates the government's ability to select content.[10] The government has substantially different interests when fulfilling these distinct roles and making these decisions.[11] The fact that there are no cases on record involving successful challenges of a library's acquisition choice demonstrates just how much deference the courts pay to the acquisition choices of libraries.[12]

---

[9] *Mainstream Loudoun v. Board. Of Trustees of the Loudoun County Library*, 24 F. Supp. 2d 552, 562 (1998).

The *Loudoun County* court also failed to understand the nature of Internet technology when it ruled that the library purchased all of the available content on the Internet when it chose to provide Internet access to its patrons. The provision of Internet access is indistinguishable from the selection of content that librarians engage in daily. By signing onto the Internet and individual has not brought the material on the Internet into the library. Rather, an individual is using the Internet to facilitate the selection of content that, once selected, will be brought into the library. The patron only selects content and brings it into the library when he or she accesses or downloads a particular site. Certainly, a patron has not selected the content of the millions of pages he or she never viewed simply because he or she signed onto the Internet.

When a state provides speech, it has no obligation to provide all speech. A state may act in a more restrictive manner when acting as a provider of speech (when the government purchases speech in order to provide it to the public) than it may when acting as a sovereign (regulating private speech on behalf of the general welfare of society).[13] There is no constitutional requirement that the government provide access to pornographic images through public libraries. An individual has a right to access legal pornography through his or her own computer but not via a publicly funded computer, and certainly does not have a right to access illegal pornography via a government-funded computer.[14] The U.S. Supreme Court has stated, "Environments such as a prison, public schools, the military, or the government workplace 'must allow regulation more intrusive than what may lawfully apply to the general public.'"[15] (Emphasis added.)

---

[10] *Kreimer v. Bureau of Police for the Town of Morristown*, 958 F.2d 1242 (1992).

[11] See *Brooklyn Inst. Of Arts & Sciences v. City of New York*, 64 F. Supp. 2d. 184, 203 (E.D.N.Y. 1999) ("Public libraries are, of physical and fiscal necessity, selective; they do not contain every book published.").

[12] Mark Nadel, *The First Amendment's Limitation on the Use of Internet Blocking in Public and School Libraries: What Content Can Librarians Exclude?*, 78 Tex. L. Rev. 1117, 1124 (2000).

Libraries that choose to provide Internet access to their patrons have not opened up a public forum. Instead, libraries have simply reserved Internet use for patrons with a legitimate research purpose consistent with the library's overall mission of providing patrons access to particular content. Rejecting the assertion that a local television channel created a public forum by deciding to air a political debate in which only certain candidates were allowed to participate, the U.S. Supreme Court stated "the Court has rejected the view that traditional public forum status extends beyond its historic confines, see *ISKCON*, *supra*, at 680-681; and even had a more expansive conception of traditional public fora been adopted, see, *e.g.*, 473 U.S., at 698-699 (KENNEDY, J., concurring in judgments), the almost unfettered access of a traditional public forum would be incompatible with the programming dictates a television broadcaster must follow."[16] When libraries choose to offer patrons Internet access, they are acting to "reserve eligibility for access to the forum to a particular class of speakers, whose members must then, as individuals, 'obtain permission,' to use it."[17] In fact, it often goes unnoticed that most libraries already restrict access to certain Internet services. Most libraries have limited Internet access policies that typically prohibit their Internet access from being used to access email accounts, chat rooms, or the Usenet groups. Furthermore, many library policies explicitly state that their resources may not be used to engage in any activity that violates federal copyright laws. It is intellectually dishonest to assert that libraries may chose not to allow patrons to access certain Internet services because they lead to a wasteful use of library resources. Equally dishonest is the assertion that libraries may take steps to prevent the use of their resources for all criminal activity *except* any activity involving obscenity, child pornography, or material harmful to minors.

---

[13] This distinction was recognized, again, by the U.S. Supreme Court in its recent decision in *NEA v. Finley*, 118 S. Ct. 2168 (1998) when it held that there is no constitutional right to government funding of the arts: "And as we held in *Rust*, Congress may 'selectively fund a program to encourage certain activities it believes to be in the public interest, without at the same time funding an alternative program which seeks to deal with the problem another way.'"

[14] In *Capital Sq. Review Bd. v. Pinette*, 115 S. Ct. 2440 (1995), the Court stated: "It is undeniable, of course, that speech which is constitutionally protected against state suppression is not thereby accorded a guaranteed forum on all property owned by the State."

[15] See *Turner v. Safley*, 482 U.S. 78, 84-85 (1987); *Connick*, 461 U.S. at 143; *Tinker*, 393 U.S. at 507; *GMC* 131 F.3d at 276. In these environments, the government is permitted to balance constitutional rights against institutional efficiency in ways it may not ordinarily do. *Waters v. Churchil*, 511 U.S. 661, 675 (describing governmental power to restrict speech in the name of efficiency; *Safley* 482 U.S. at 88 (Noting balancing between First Amendment rights and governmental interests.)" *Amatel v. Reno*, 156 F.3d 192 (1999) *cert. denied*, 67 U.S.L.W. 3781 (1999).

Regardless of the intellectual content libraries offer, all libraries seek to provide efficient, quality access to material.[18] In doing so, libraries must exercise discretion when selecting particular works in order to fulfill this goal. Certainly the conclusion that libraries must offer "broad rights of access for outside speakers" with regard to the selection of content is antithetical to the general purpose of libraries to provide efficient access to the highest quality of use material.[19]

---

[16] *Arkansas* at 679

[17] *Id.*

[18] Nadel at 1138.

[19] *Arkansas* at 674.

Librarians have always chosen not to select material that is inconsistent with their vision of their obligation to provide a service to their patrons. Librarians will generally decline to purchase materials that they conclude are factually inaccurate or filled with misinformation. By choosing to do so the library has not prohibited the dissemination of such materials and patrons wishing to review such materials are free to purchase those works as consumers or to access it on a privately owned computer. The First Amendment does not prohibit libraries from using reasonable nonpartisan standards to exclude content that it finds to be "defective" just as it does not prohibit public museums from excluding what they, in their professional judgment, believe to be "bad" art.

Libraries omit XXX-rated material from their collections, despite its popularity with some patrons. Most librarians probably do not consider sexually materials designed merely for prurient purposes to be within the scope of their goals, even if such photos are clearly not obscene. When allocating their limited budgets, most have no difficulty declining subscriptions to XXX-rated magazines and similar material. Such decisions have gone unchallenged.

Blocking Technology is an Effective Method of Restricting Minors' Access to Illegal Pornography in Public Libraries

Opponents of the use of blocking technology in public libraries argue that the technology is an ineffective method of preventing children from accessing pornography and adults from accessing obscenity and illegal pornography. This argument is outdated and insincere.

A library's inability to provide a selection of all known literary works is a problem faced by librarians and library patrons daily. When a book of choice is not available in a public library, there are a number of options a patron may pursue in order to obtain that book. Traditionally, the patron will ask the librarian to do a search for the piece. If the book has been checked out, a patron may wait up to a month before obtaining a copy of the book. If the library does not carry the book, the patron has the option of borrowing a copy from another library through an interlibrary loan. If neither of these options work, the patron must pursue other options for obtaining the book. In practice, the use of blocking technology in a library is very similar to this selection process.

As blocking technology has evolved, both server and user based technology has responded to consumer needs and are highly effective at blocking pornographic material while allowing for the selection of legitimate research materials.[20] A recent report released by FRC titled *Dangerous Access, 2000 Edition: Uncovering Internet Pornography in America's Libraries*, revealed that those libraries that do employ blocking technology on their Internet accessible computers have encountered little to no patron dissatisfaction with the technology and a minute number of incorrect blocks. A 1998 survey of twenty-four public library administrators who use filters found on 1.6 complaints per month alleging wrongly blocked sites.[21] According to *Dangerous Access*, the logs of Tacoma, Washington indicate that only 0.07 percent of the sites blocked there were incorrectly blocked and in Cincinnati, Ohio only 0.01 percent were incorrectly blocked.[22]

---

[20] On July 20, 2000, the Commission heard testimony from panelists addressing the "Effectiveness of Filtering, Labeling and Rating Technologies."
[21] David Burt, *Dangerous Access, 2000 Edition: Uncovering Internet Pornography in America's Libraries*, Family Research Council 38 (2000).
[22] *Id.*

In order to investigate the effectiveness of blocking technology for my own satisfaction, I performed my own Internet search on my FRC owned computer. FRC uses blocking software manufactured by "Surf Watch." Attached to my testimony is an appendix containing the results of this search. A search of "breast augmentation" on WebCrawler brought back 14,457 results and my search of "penile implants" brought back 2,387 results. Under both categories I was able to access sites that provided detailed descriptions of various procedures including full color before and after photographs from successful patients. In addition, my search of "Essex" brought back 5,361 results, "Woodcock" 706 results, a photograph of Michelangelo's David, and a full listing of all of Shakespeare's works within which the term "breast" appears.

It is my opinion that the First Amendment would prohibit librarians from abdicating complete responsibility for final access decisions to a private third party, which will not be subject to First Amendment constraints. However, by working closely with companies providing blocking services to obtain a list of blocked sites or the criteria by which blocking companies chose to block a particular category of Websites, librarians can ensure that they maintain final control over content selection so as to prevent any unreasonable restrictions on content or viewpoint discrimination.

Moreover, even if a site is incorrectly blocked virtually all companies that provide blocking services will unblock a site upon request within 24 to 48 hours. A patron, however, can usually receive immediate assistance from the librarian on duty. All blocking services allow for the user, usually with some type of password or special identification, to override the product's instructions to block a particular site. In the event that a patron's attempt to access a legitimate research site is thwarted by an incorrect blocking instruction, that patron need only file a request with the librarian on duty to have the site unblocked. Such requests are usually complied with within minutes of having been registered. Furthermore, opposition arguments that blocking technology blocks out whole websites with valuable content due to some "inappropriate" pages is indistinguishable from a librarian's choice not to purchase printed books and magazines with valuable content because they also include "inappropriate" material. Absolute perfection is not, nor has it ever been, required under the First Amendment.

Public Libraries Have Numerous Compelling Interests Justifying The Use of Blocking and Blocking Technology on Its Internet Accessible Computers

There is no doubt that libraries, whether they are adjudged to be a traditional, limited public forum, or a non public forum, may choose not to provide access to content that does not receive protection under the U.S. Constitution such as obscenity, child pornography, material created in violation of copyright laws, or defamatory speech. Furthermore, as a nonpublic forum, libraries exercising their discretion to select materials for inclusion in its collection may restrict speech that does receive protection under the First Amendment because the forum has not been opened up for the benefit of third party speech. If courts reach the appropriate legal conclusion that libraries are not a public forum, the analysis could and would stop at this point. However, even if the Internet were to be ruled a limited public forum, the are numerous compelling interests justifying a library's decision to place blocking and blocking technology on Internet accessible computers to block access to illegal pornography.

Government Has A Compelling Interest in Eliminating Obscenity and Child Pornography

The U.S. Supreme Court has consistently held that the First Amendment does not

> protect obscenity and child pornography. "The lewd and obscene, the profane, the libelous, and the insulting or 'fighting' words … are no essential part of any exposition of ideas, and are of such slight social value as a step to truth that any benefit that may be derived from them is clearly outweighed by the social interest in order and morality."[23]

There is no right to publicly and commercially disseminate or exhibit obscene materials, even though private possession in one's own home is protected. Furthermore, the Court has clearly state that any rights of possession existing in one's home does not follow that individual out of the home, "we have declined to equate the privacy of the home … with a 'zone' of 'privacy' that follows a distributor or a consumer of obscene materials wherever he goes. … Conduct or depictions of conduct that the state police power can prohibit on a public street do not become automatically protected by the Constitution merely because the conduct is moved to a bar or a 'live' theater stage, any more than a 'live' performance of a man and woman locked in a sexual embrace at high noon in Times Square is protected by the Constitution because they simultaneously engage in a valid political dialogue."[24] The Court's conclusion was based upon its concern that public dissemination of obscenity carries with it the danger of offending the sensibilities of unwilling recipients or exposure minors to such material, "public distribution of obscene materials … is subject to different objections. For example, there is always the danger that obscene material might fall into the hands of children, see *Ginsberg* v. *New York, supra*, or that it might intrude upon the sensibilities or privacy of the general public."[25] The Court has also held that consenting adults do not enjoy any right to receive, transport, or distribute obscenity even if for private use or not for commercial or pecuniary gain.[26] The *Loudoun County* court also recognized the government's compelling interest in preventing the distribution of obscenity and child pornography and in preventing the creation of a hostile environment in violation of federal sexual harassment laws.[27]

---

[23] *Chaplinsky v. New Hampshire*, 315 U.S. 568, 172 (1942). In *Miller v. California*, 413 U.S. 15, 24-25 (1973), the U.S. Supreme Court announced the constitutional test and definition for obscenity currently used by federal law and most state laws. The test seeks to address three possible qualities of speech: whether the material appeals to the prurient interest; depicts sexual conduct in a patently offensive way; and lacks serious literary, artistic, political, or scientific value. "The case also categorically reaffirmed that obscene materials are not protected speech, recognized that the States have a legitimate interest in criminalizing the dissemination or exhibition of obscene materials and could use community standards as a measure of the views of the average person for the prurient and patent offensiveness findings of fact." National Law Center for Children and Families, National Law Center Memorandum of Law On Legal Issues Involving Use of Filtering Software By Libraries, Schools and Business to Screen Acquisition of

The Court recently affirmed the constitutionality of the enforcement of federal obscenity and child pornography statutes in cyberspace.[28] "Transmitting obscenity and child pornography, whether via the Internet or other means, is already illegal under federal law for both adults and juveniles."[29] It's particularly instructive that the Court relied upon blocking technology as a possible means of the government achieving its interest of protecting children from material harmful to minors. "By contrast, the District Court found that "despite its limitations, currently available *user-based* software suggests that a reasonably effective method by which *parents* can prevent their children from accessing sexually explicit and other material which *parents* may believe is inappropriate for their children will soon be widely available.'"[30]

Pornographic Material From the 'Internet' is Both Lawful and Constitutional 10 (1997) [hereinafter Law Center].

[24] *Paris v. Slanton*, 413 U.S. 49, 66,67 (1973).

[25] *Stanley v. Georgia*, 394 U.S. 557, 567 (1973) (holding that possession of obscene material cannot be prohibited in one's residence). (The court was distinguishing the private, secluded nature of the home from the public.)

[26] *U.S. v. Orito*, 413 U.S. 139, 141-42 (1973).

[27] *Mainstream Loudoun v. Bd. of Trustees of the Loudoun County Library*, 24 F. Supp. 2d 552 (1998).

[28] *Reno v. ACLU*, 521 U.S. 844, at 877 n.44 (1997).

[29] *Id.*

[30] *Reno* at 844

Unlike obscenity, the mere possession of child pornography, in addition to the production, receipt, transportation and distribution of child pornography are prohibited.[31] Concerning child pornography, the Court has concluded, "materials produced by child pornographers permanently record the victim's abuse. The pornography's continued existence causes the child victims continuing harm by haunting the children in years to come" and that "encouraging the destruction of these materials is also desirable because evidence suggests that pedophiles use child pornography to seduce other children into sexual activity."[32] Of child pornography the Court has stated, "The prevention of sexual exploitation and abuse of children constitutes a government objective of surpassing importance … the distribution network for child pornography must be closed if the production of material which requires the sexual exploitation of children is to be effectively controlled."[33]

In addition to U.S. Supreme Court precedent, federal law prohibits the transportation (including the mailing[34]), sale, distribution and receipt of obscene material;[35] possession with intent to sell, and sale, of obscene material on federal property;[36] the transportation, shipping, receipt and distribution of child pornography; the sale or possession with intent to sell of child pornography; and the knowing possession of visual depictions of child pornography made in whole or in part of materials transported in interstate or foreign commerce.[37] Furthermore, most state laws make it illegal to use computer transmissions to disseminate, exhibit, or distribute obscenity within a state. Finally, all states criminalize the distribution, dissemination, and exhibition of child pornography and most prohibit possession, as well. Libraries and educational institutions utilizing "interactive computers services" could be found to be subject to the provisions of these laws.[38]

---

[31] *New York v. Ferber*, 458 U.S. 747 (1982). Child pornography is defined as follows: An unprotected visual depiction of a minor child (federal age is under 18) engaged in actual or simulated sexual conduct, including a lewd or lascivious exhibition of the genitals. See *New York v. Ferber*, 458 U.S. 747 (1982), *Osborne v. Ohio*, 495 U.S. 103 (1990), *U.S. v. X-Citement Video, Inc.*, 115 S. Ct. 464 (1994). See also *U.S. v. Wiegand*, 812 F.2d 1239 (9th Cir. 1987), *cert. denied*, 484 U.S. 856 (1987), *U.S. v. Knox*, 32 F.3d 733 (3rd Cir. 1994), *cert. denied*, 115 S. Ct. 897 (1995). In 1996, 18 U.S.C.§ 2252A was enacted and § 2256 was amended to include child pornography that consists of a visual depiction that is or appears to be of an actual minor engaging in sexually explicit conduct. See *Free Speech Coalition v. Reno*, No. C-97-0281 SC, judgment for defendants, Aug. 12, 1997, unpublished, 1997 WL 487758 (N.D. Cal 1997).

[32] *Osborne at 111.*

[33] *New York v. Ferber*, 458 U.S. 747, 757 (1982).

[34] 18 U.S.C. § 1461 (1999).

[35] 18 U.S.C. §1462 (1999), 18 U.S.C. § 1465 (1999).

[36] 18 U.S.C. § 1460 (1999).

There is a Constitutional Mandate to Prevent Children From Accessing Material Harmful to Minors

The U.S. Supreme Court has consistently recognized society's "compelling interest" in protecting minors from sexually explicit material defined as "harmful to minors." The societal availability of pornography erodes public standards of morality affecting all members of the community and in particular children. In *Ginsberg v. New York*,[39] the U.S. Supreme Court recognized the observations of psychiatrist Dr. Gaylin of the Columbia University Psychoanalytic Clinic, reporting on the views of psychiatrists in 77 Yale Law Journal at 592-593:

> 'Psychiatrists ... made a distinction between the reading of pornography, as unlikely to be per se harmful, and the permitting of the reading of pornography, which was conceived as potentially destructive. The child is protected in his reading of pornography by the knowledge that it is pornographic, i.e. disapproved. It is outside of parental standards and not a part of his identification process. To openly permit implies parental approval and even suggests seductive encouragement. If

---

[37] 18 U.S.C. § 2252 (1999).
[38] Law Center, supra note 23, at 39.

> this is so of parental approval, it is equally so of societal approval – another potent influence on the developing ego.'

States criminalize disseminating harmful "soft-core" pornographic material to minors, even though the material may not be obscene for adults[40] and governmental regulations may also act to facilitate parental control over children's access to sexually explicit material.[41] The Court has ruled that, "constitutional interpretation has consistently recognized that the parents' claim to authority in their own household to direct the rearing of their children is basic in the structure of our society. 'It is cardinal with us that the custody, care and nurture of the child reside first in the parents, whose primary function and freedom include preparation for obligations the state can neither supply nor hinder.'"[42]

The most recent U.S. Supreme Court case to address congressional efforts to regulate sexually explicit material in order to protect children, *Reno v. ACLU*,[43] left the right of states to enforce such "harmful to minors" laws undisturbed. In Reno, the Court reiterated its prior definitive holdings that protecting children from exposure to obscene and harmful material is a matter of "compelling" and "surpassing" state interest.[44] This area of the law is quite settled, as evidenced by the fact that there are very few prosecutions for providing harmful matter to minors, because convenience stores, video stores, theaters, and even "adult" porn shops comply with state "harmful to minors" and display laws.[45]

Most states have enacted "harmful to minors" legislation, patterned after the New

---

[39] 390 U.S. 629, at 642, n.10 (1968).
[40] *Id.*
[41] See *Action for Children's Television v. FCC*, 932 F.2d 1504 (D.C. Cir. 1991), *cert. denied*, 112 S. Ct. 1282 (1992); and *Sable Communications v. FCC*, 492 US 115 (1989).
[42] *Ginsberg* at 639.
[43] *Reno*.
[44] Law Center, *supra* note 23, at 40.
[45] *Id.*

York statute upheld by the U.S. Supreme Court in *Ginsberg v. New York*,[46] which placed controls on the dissemination of "harmful matter" to minors even though that matter may not be obscene for adults. In *Ginsberg*, the Supreme Court definitively held that the scope of the constitutional freedom of expression secured to a citizen to read or see material concerned with sex can be made to depend on whether the citizen is an adult or a minor; that protecting children from exposure to obscene or harmful material satisfies a compelling state interest; and that parents and others who have the primary responsibility for children's well-being are entitled under the U.S. Constitution to receive the support of laws designed to aid discharge of that responsibility.[47]

The Court has also held that obscene Dial-a-Porn may be banned from phone systems,[48] and indecent Dial-a-Porn may be regulated by credit cards, access codes, or subscription so as to avoid access by minors.[49]

The Legal Effects of Failing to Filter out Pornography

By distributing illegal material at taxpayer expense, public schools and libraries are creating contempt for the laws under which private individuals may be prosecuted. Under the legally recognized test to determine whether material is "obscene"[50] or "harmful to minors," that material must be judged in light of community standards. "Community standards" are determined in the community from which the jury pool is drawn. Each juror is presumed by law to know what the views of the average or reasonable person are (in the same way that jurors in civil cases are held to know what constitutes "reasonable" conduct under the "reasonable person" standard for negligence, and so on). Failure to keep pornography out of libraries may result in sexually oriented businesses pointing to its availability in local public libraries as proof that their own material is now "accepted" in a community.[51] Recently, the publisher of a pornographic magazine in Arizona used this very argument to defend against his arrest for distributing material harmful to minors in violation of a state law prohibiting the distribution of material harmful to minors via sidewalk vending machines that are accessible to minors. He argued that the Phoenix Public Library

---

[46] 390 U.S. 629 (1968). Harmful to minors is defined as any written, visual, or audio matter of any kind that: 1) the average person, applying contemporary community standards, would find, taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; 2) the average person, applying contemporary community standards, would find depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, ultimate sexual acts, normal or perverted, actual or simulated, sado-masochistic sexual acts or abuse, or lewd exhibitions of the genitals, pubic area, buttocks, or post-pubertal female breast; 3) a reasonable person would find, taken as a whole, lacks serious literary, artistic, political, or scientific value for minors. As with obscenity, in order to be found to be material harmful to minors, material must meet all three of these individual tests. Law Center *supra* note 23, at 7.

[47] Law Center, *supra* note 23, at 40.

[48] *Sable Communications v. FCC*, 492 U.S. 115 (1989). 492 U.S. at 124-26.

[49] *Sable*, 492 U.S. at 121-22, 128-31.

[50] Obscenity is determined using the following test: 1) Whether the average person, applying contemporary adult community standards, would find that the material, taken as a whole, appeals to a prurient interest in

> has materials available for minors which are infinitely more graphic than Defendant's newspaper. … A Comparison between Defendant's newspaper and materials the State itself has available for minors for free proves that the State's standards tolerate material which is infinitely more 'patently offensive' in terms of the written word, pictures and/or images evoked than anything in Defendant's newspaper.[52]

---

sex (*i.e.*, an erotic, lascivious, abnormal, unhealthy, degrading, shameful, or morbid interest in nudity, sex, or excretion); 2) Whether the average person, applying contemporary adult community standards, would find that the work depicts or describes, in a patently offensive way, sexual conduct (*i.e.*, ultimate sex acts, normal or perverted, actual or simulated; masturbation; excretory functions; lewd exhibition of the genitals; or sadomasochistic sexual abuse); 3) Whether a reasonable person would find that the work, taken as a whole, lacks serious literary, artistic, political, or scientific value. In order to be found obscene, material must meet all three of these individual tests. Law Center *supra* note 23, at 7.

[51] Janet M. LaRue, Statement at Press Conference Introducing The Children's Internet Protection Act (March 2, 1999).

[52] *Defendant's Motion for Determination that the Newspaper in Question Is Not "Harmful to Minors,"* November 21, 1997 (visited June 29, 1999), http://blockingfacts.org/everson.htm.

The viewing of pornography in public places creates an "offensive, uncomfortable, and humiliating environment for women co-workers" and can "constitute or be evidence of sexual harassment in violation of state and federal civil rights laws and create or contribute to a hostile enforcement in violation of Title VII's general prohibition against sexual discrimination in employment practices." Businesses and offices, public and private, are constrained by various federal and state laws, with respect to conduct in the workplace, and the duty to take affirmative steps to eradicate workplace discrimination. The eradication of workplace discrimination is more than simply a legitimate governmental interest, it is a compelling governmental interest. State and federal governments have a compelling interest in eliminating discrimination against women by removing barriers to their economic, political, and social advancement within our culture.[53] In addition to its connection to crimes against women, pornography demeans and objectifies women by reducing their worth to nothing more than a tool for male sexual gratification.

Libraries making good faith use of blocking and blocking technology to prevent children from accessing obscenity and material harmful to minors, and adults from accessing obscenity, are protected from civil liability by the "Good Samaritan" immunity, provided by federal law.[54] (The "Good Samaritan" immunity also extends to civil protection from suits by those who would try to force an institution to carry its material, even if that material is "protected.") Libraries are specifically provided immunity as providers or users of interactive computer services for "any action voluntarily taken in good faith to restrict access or availability of material that the provider or user considers to be obscene ... excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected." The law also protects an ISP, online service, or institution that filters out or restricts access to certain "hate speech" or other offensive pornographic or violent materials so as not to assist those speakers, even though their message would be available otherwise on the Web or in newsgroups.[55] Such filters could also provide a criminal law defense against the "knowing" transmission of illegal pornography inadvertently or deliberately accessed.

---

[53] Law Center, *supra* note 23, at 32.
[54] 47 U.S.C. § 230(c)(2)(A).

Conclusion

The revolutionary power of the Internet is undoubtedly one of the most important developments of the 20th Century. Its vast reach makes information once contained in isolated; distant locations accessible to millions of children at their local libraries, schools, or home. Most parents deeply desire for their children to take part in this revolution. The Internet has also quickly become the favorite tool of criminals, including pornographers, due to its quick and easy access and the absence of a strong law enforcement presence. It's no secret to children or adults that the most violent, offensive, and graphic forms of pornography are also readily available. Despite U.S. Supreme Court rulings affirming the applicability of federal obscenity and child pornography laws to the Internet, pornographers are well aware that the number of prosecutions of Internet crimes is substantially lower than the same crimes committed through other venues. In the absence of vigorous law enforcement efforts aimed at removing illegal pornography from the Internet, it is essential that parents receive assistance as they try to prevent their children from accessing material that would be illegal for them to access outside of a public library.

---

[55] *Id.*

BRIEF BIOGRAPHICAL DATA OF

COLBY M. MAY

COLBY M. MAY is Director, Office of Governmental Affairs, of the American Center for Law and Justice, a nonprofit, public interest law firm and educational organization. ACLJ attorneys have argued and participated as amicus curiae in several landmark cases at the Supreme Court, including *Lamb's Chapel v. Center Moriches Union Free School District*, 113 S.Ct. 2141 (1993); *Bray v. Alexandria Women's Health Clinic*, 113 S. Ct. 753 (1993); *United States v. Kokinda*, 497 U.S. 720 (1990); *Board of Education v. Mergens*, 496 U.S. 226 (1990); *Frisby v. Schultz*, 487 U.S. 474 (1988); and *Board of Airport Commissioners v. Jews for Jesus*, 482 U.S. 569 (1987), *Santa Fe Independent School District v. Doe*, (S.Ct. Dkt. 99-62); *Hill v. Colorado*, (S.Ct. Dkt. 98-1856), *Troxel v. Granville* (S.Ct. Dkt. 99-138); *Mitchell v. Helms* (Sp. Ct. Dkt. 98-1648); *Schenck v. Pro-Choice Network of Western New York*, 519 U.S. 955 (1997); *National Endowment for the Arts v. Finley*, 522 U.S. 1105 (1998); and *Turner Broadcasting Systems, Inc. v. FCC*, 512 U.S. 622 (1994). Mr. May has over 20 years experience in federal litigation and federal regulatory agency proceedings. Before joining the American Center for Law and Justice, he was a partner with the communications firm of May & Dunne, Chartered, which specialized in representing broadcast clients before the Federal Communications Commission. He has conducted numerous seminars on how to comply with the FCC's broadcast rules, including its EEO and Affirmative Action requirements. Mr. May also specialized in representing nonprofit, tax-exempt organizations. He is a member of the District of Columbia Bar; Virginia State Bar; Federal Communications Bar Association; Federal Bar Association; National Association of Broadcasters; and Phi Delta Phi (Historian, 1977-79), and is admitted to practice before the U.S. District Court, Eastern District of Virginia; the United States Court of Appeals, Fourth Circuit; the Supreme Court of Virginia; the U. S. Claims Court; the U. S. Court of Appeals, District of Columbia Circuit; the District of Columbia Court of Appeals; the U.S. District Court for the District of Columbia; and the Supreme Court of the United States of America. Mr. May is a graduate of George Mason University, School of Law (J.D., 1980) and Stetson University (B.A., 1975). He has also served on the board of directors of many civic organizations and currently serves as a director and Secretary of Enterprise Development International, Inc., a public charity fostering micro-economic development in emerging countries of the world.

Policy Implications of Filtering, Labeling, and Rating

COPA COMMISSION FIELD HEARING
Panel Seven
Richmond, Va. July 21, 2000

Colby M. May
Director, American Center For Law and Justice

I. Introduction:

While the vital movement to protect children from online exposure to detrimental pornography has received another recent setback in the 3rd Circuit (ACLU v. Reno III)[1], it is important to recognize that ample support remains in the Courts of official jurisdiction and public opinion to achieve this objective. Contrary to the picture painted by constitutional contortionists, the **First Amendment grants us the liberty to protect our children** from exposure to harmful material they are not prepared for **without depriving them** of access to the ample educational and cultural **benefits of the Internet** or the **privileges of a free society.** In addition, providing this selective protection does not consequently relegate adult choices to only that which is suitable to children.

II. Compelling Interests and Concerns

a. The Inherent Government Interest

The Supreme Court has established that "the **government has a compelling interest** in protecting the physical and psychological well-being of minors from the adverse effects of pornography." (Ginsberg v. NY)[2] This interest includes the efforts to **shield minors from the influence of categorically non-obscene literature** by adult standards, (Sable Comm. v. FCC)[3] as well as other common forms of free expression.

---

[1] 2000 WL 801186 (3rd Cir. (Pa.))(affirming the District Court's grant of a preliminary injunction in "confidence" of its unconstitutionality)

[2] 390 U.S. 629, 639-640 (1968) (also adding that the government had an interest in supporting "parents' claim to authority in their own household" in justifying the regulation of otherwise protected expression)

[3] 492 U.S. 115, 126 (1988)

b. +/- of the Internet

The Internet is a welcome, invaluable educational and cultural resource. Like broadcasting and literature, it is easily accessible to children. (though it also avails itself to those too young to read.) The Internet, however, is also widely recognized as a global forum for variants of exploitive, vulgar, and indecent material that are neither instructive nor beneficial for minors.

c. Is There Really a Problem?

Opponents believe that panels such as these ideally wouldn't be necessary, because at root **they don't feel that a problem even exists.**[4] Some typically infer that religiously motivated fringe groups are once again orchestrating a **paternalistic "obsession with indecency and porn**." The reality is that concern for children's exposure to the plethora of pornography on the Web is a **bi-partisan, mainstream, majority movement** embraced by a multiplicity of cultural and religious perspectives.[5] The harmful effects of pornographic exposure on minors have long been recognized by librarians, educators, and the fields of medicine and psychology. They also have received noteworthy attention from the Surgeon General (1986 report) and the White House (1997).[6]

---

[4] Lawrence Lessig, What Things Regulate Speech: CDA 2.0 vs. Filtering, 38 Jurimetrics J. 629, 633. (1998) "I am not now advocating a CDA 2.0 -like solution because I believe that there is any real problem (of child access to Internet porn). In my view (ideally), it would be best if things were just let alone...My view is that nothing is better than something."

[5] The commentary from Lessig and the ACLU denying any "problem" is astounding. Over the last couple of years, articles have flooded the country's newspapers with complaints from parents and librarians. Just one example, in Minneapolis (MN.), librarians have made a sex-discrimination claim against the library with the EEOC charging that youths' access to Internet sex sites has created an indisputably hostile, offensive, and palpably unlawful working environment." (Newsweek, July 8, 2000)

[6] Last December's White House initiated Internet Online Summit: Focus on Children was an explicit recognition of the breadth of concern for Internet pornography and predation and its effects

A recent "Hardball" episode with Chris Matthews of MSNBC (07/13/00, discussing the cultural ramifications of the populace's mounting passion for Internet porn) revealed an Austin, Texas-based poll showing that on average, one third **(32.7%)of all Internet users are logged onto pornographic sites at any given time**. Certainly, there is no legal issue at face value in this statistic, as long as these sites steer clear of constitutionally recognized obscenity and/or child pornography. The number does become more morally problematic, and legally remediable, when you begin to postulate the **percentage of minors included in that figure**. Parents have indicated that they would like to see our leaders mobilize to address the issue, as evidenced by numerous news reports on the subject over the last few years and by their support for the trail of federal, state, and local attempts to regulate children's exposure to the indecent "negative externalities" of the 'Net.

d. Libraries Share in this Interest

Inherently, Public Libraries, share the State's duty in safeguarding the physical and psychological well-being of minors from any such harmful material (see NY v. Ferber).[7] It is in this context, the protection of children in their formative years, that libraries may constitutionally use filtering systems or designate certain terminals with filtering software. In absence of such devices, libraries may become liable for the inevitable harm to innocents exposed to pornography for the first time.

III. Filtering Devices are Reasonable, Necessary, and not Viewpoint Discriminatory

a. Recent Case Law Favors Constitutionality of Filtering

Opponents have pointed to the recent Mainstream Loudoun v. Bd. of Trustees of the Loudoun County Library [8] lower court decision in arguing the unconstitutionality of library filtering. The opinion, innately narrow and highly contextual, has been overruled in principle by the 4th Circuit decision in Urofsky v. Gilmore, [9] which held that **restrictions** on viewing Web based sexually

---

on children. See Bruce Watson of Enough is Enough, "Public Hearing: National Commission for Library Information and Science", (11/10/98)

[7] 458 U.S. 747, 756-758 (1982) (holding child pornography an unprotected form of speech)

[8] 24 F. Supp.2d 552 (1998)

[9] 1999 WL 61952 (4th Cir. (Va.)) (02/10/99)

explicit material for state employees (on state owned or leased terminals) **were constitutionally valid**.

b. The Loudoun decision can also be criticized for its erroneous classification of public libraries as "limited public forums." Recent related cases, such as General Media Comm. v. Cohen,[10] have rendered similar government-sponsored facilities either as nonpublic forums or **facilities where aesthetic decisions are allowed to be made for collection and distribution of material**. In this setting, the government may enact and enforce "time, place, and manner regulations, [to]...reserve the forum for its intended purposes, communicative or otherwise, as long as the regulation on speech is reasonable and not an effort to suppress expression because public officials oppose the speaker's view." (Perry Educ. Ass'n v. Perry Local Educator's Ass'n)[11]

c. Filters Continue the Library's Tradition of Excluding Pornographic Material from Minors

In recognizing the **library's tradition of content-based selection and exclusion**, the fact that public libraries do not carry the likes of *Hustler* and *Deep Throat* indicates that they **do not regard this material to be within their mission of open access** to information.[12] Consequently, libraries **should be equipped** to maintain this levelheaded policy of **restricting minors' access to such items as any new medium** for them develops.

d. The Court has upheld as a reasonable limitation, restrictions of broadcasts of political candidates and their platforms, for example, in the considerations of "educational value and the public interest."(see Arkansas Educ. Television Comm. v. Forbes)[13] Similarly, ensuring that certain pornographic material is not accessible to children at computer terminals by **utilizing filtering devices is a reasonable function** for a library in **service of the "public interest, educational value, and convenience**." Libraries are not open forums by government designation, but instead are government agencies which **can exercise editorial discretion with their purchasing power**. (See NEA v. Finley)[14]

---

[10] 131 F. 3d 273, cert. denied, 118 S. Ct. 2637 (1998)

[11] 460 U.S. 37, 45 (1983)

[12] Filtering Facts, Responses to Arguments Against Filtering, <http://www.filteringfacts.org/resp.htm>

[13] 118 S. Ct. 1633 (1998) (Emphasizing that editorial discretion may be exercised by a governmental agency procuring art)

[14] Id at 2168.

e. Filters are Effective and Not Overly Restrictive

Even though libraries are not necessarily compelled to use the least restrictive means to accomplish this goal, **filtering software just happens to be the least restrictive (effective) instrument** to block harmful material currently available. The **alternatives** advocated by the American Library Association and the ACLU: (1) Acceptable Use Policies for parents, teachers, and librarians, (2) Time Limits, (3) Driver's Ed for the Web, (4) Recommended Reading, (5) Privacy Screens, etc...**rely merely on education, time limits, and even privacy screens** to accomplish the goal. These procedures fail, however, since they ignore the reality of prepubescent curiosity and recalcitrance, the abundance of "copycat" or "stealth" porn sites which are designed to trap innocent users, and overall, tend to **only limit the** *amount* **of pornography exposure without addressing the main issue of** *access*.

f. Opponents have criticized filters for their propensity to over exclude and consume the limited time of library officials. In response, 1) it is important to weigh the harm that results from minimal, easily correctable levels of product imperfection versus the potentially devastating effects on thousands of lives as a result of their interaction with obscenity and female exploitation in the absence of such mechanisms. In a 1998 survey of 24 random libraries (who bucked threats of ACLU driven suits to participate), only 3.6 hours of librarian commitment was needed for implementation of terminal filters per month and only 1.6 complaints (per month) about excessive filtering were made by adults (the latter # significantly was effected by a suspicious number of filings at one particular Austin, TX facility). 2) In addition, it is spurious to suggest that perfect results are a prerequisite for legislative remedy.

g. Alternatives are More Problematic and Less Effective

To advocate the implementation of filtering software is not to discourage research and investigation of other means to address the issue. Several Court members, specifically Justice O'Connor in her separate concurrence in the Reno v. ACLU case,[15] have suggested that ***Internet zoning*** would be constitutional as long as it maintained the freedom of adult users to gain access to protected speech. Opponents have expressed concern that versions of these programs, such as "kid friendly Internet services" that only allow access for children controlled by the service provider, **would also limit the amount of educational information available** for children.

Age verification devices **also present a constitutionally sound route**. They would require adult Web sites to bar entry to adult sites without proof of age via either a credit card number or an electronically signed statement. There are,

---

[15] 521 U.S. 844, 886 (1997) (O'Connor, J., concurring in part, dissenting in part).

however, some problems with this method. For one, they **assume no transaction costs**. Besides imposing a **significant financial burden** on adult sites, it has been pointed out that even if administrative costs could be externalized, **noncommercial providers may not be able to afford the setup**, perhaps validating one of the Supreme Court's concerns about discriminatory results in the original Reno case.[16] Proposals for government sponsored devices would palpably prove to be overly expensive, bureaucratic, and intrusive. In addition, **AVSs would not be foolproof.** Once a password is given, it is subject to shared copies, not to mention the fact that many **kids today have been given access to their parents credit** cards (often specifically for the purpose of online purchasing).[17]

Rating systems alone (as opposed to the PICS application) would not be as effective on the Internet as in other arenas (films etc.), since **access would still be possible** despite notification of indecency and obscenity.

An estimated 85% of public libraries already have "***acceptable use policies***" as well, and yet there are still hundreds of examples of children's access to pornography. Neither do such policies protect kids from the proliferation of those "stealth" porn sites. (E.g. Search phrase "Pokemon pictures" would yield an irreversible entrance into a porn site where images of vaginal, oral, and anal sex is clearly visible)

h. Filters are not Viewpoint Based Restrictions

To pass Constitutional muster with the present Court, any action taken will not only need to demonstrate reasonability but **viewpoint neutrality** and general honoring of accepted First Amendment principles. Clearly, Internet filtering accomplishes these objectives since obligations tied to the eligibility for e-tax dollars, for example, would be constitutional based on selectivity for "activities it believes (or doesn't believe) to be in the public interest" (see Rust v. Sullivan)[18], in contrast to distinction founded on the "specific premises, perspectives, and standpoints...for discussions." (see Rosenberger v. Rector for the Court's definition of viewpoint discrimination)[19] The Court has already concluded that **distinctions for obscenities, offensive in their "prurience" and**

---

[16] Christopher Turlow, "Erogenous Zoning on the Cyber-Frontier," 5 Va. J.L. & Tech. 7, 50 (2000)

[17] Elizabeth M. Shea, "Is Internet Filtering Software the Answer?" 24 Seton Hall Legis. J. 167, 200

[18] 500 U.S. 173, 193 (1991)

[19] 515 U.S. 819, 829 (1995)

"lasciviousness" are not viewpoint discriminatory. (See, e.g., Bd. of Educ. v. Pico)[20] Internet Filtering also can be implemented so as not to "unduly restrict adults" access to constitutionally protected speech by allowing libraries to separate terminals for adults and children. As even the **Loudoun opinion implied, such a procedure would have been a constitutionally less restrictive alternative to the policy presented in that case (filtering devices on *all* computers)**.[21] In addition, government funding can be tailored to control the gateway of accessibility to the Internet for children, and to **avoid controlling the web itself as a means of expression**. (as opposed to the interpretation of the CDA, struck down in ACLU v. Reno in 1998).

i. The Children's Internet Protection Act 1999 [22] would have withstood constitutional scrutiny since it; 1) only required compliance if a library wanted to receive e-rate funding, 2) it did not regulate the posting or transmission of content on the 'Net but, rather, blocked the receiver, enabling publishing of protected speech to continue, 3) it avoided setting a national standard for "harmful" speech, and allowed local communities flexibility to select their own choice of filtering software and to remove the devices if they chose.[23]

IV. Conclusion

It is interesting that **screening software was once widely anticipated** as the technological development that would eventually pacify the interests of both First Amendment guardians and concerned citizens. (See 39 Catholic Law Review 125, 151 (Fall 1999) ACLU attorneys had even referred to filter use as a less restrictive device in the first of the trilogy of ACLU v. Reno cases regarding the CDA.) The vigorous opposition which has now been exhibited against this effective and minimally restrictive instrument **exposes their radical and counterintuitive agenda**. In her book, *Defending Pornography*, ACLU President Nadine Strossen quotes with approval a writer's observation that:

---

[20] 457 U.S. 853, 871 (1982) The removal of books from public school libraries because of their "pervasive vulgarity" would be permissible whereas removal of books because of their "ideas" would not.

[21] Loudoun, 24 F. Supp.2d at 552.

[22] S. 97, 106th Congress (1999)

[23] S. 97 106th Congress. Last Action: Placed on Senate Legislative Calendar under General Orders. Calendar No. 262

"Pornography tells me...that *none* of my thoughts are bad, that anything goes."[24] The **same organization** also publicly **believes that any law** which "punishes the distribution or exposure of obscene, pornographic, or indecent material to *minors* **violates the First Amendment**. (ACLU Policy 4 (b), but see Ginsberg v. New York) This position **starkly contrasts that of the Court**. It has declared obscenity, and specifically child pornography, as "harmful to the physiological, emotional, and mental health of the child." (Ferber at 756-758), and also that classes of obscenity protected for adult viewing (indecent material) are subject to regulation for minors' viewing. (Ginsberg v. NY) The Court has also stated the belief that "during the formative years of childhood and adolescence, minors often lack the experience, perspective, and judgment to identify and avoid choices that could be detrimental to them." (Bellotti v. Baird)[25]

To deny legislative support for Internet filtering devices is to allow our Public Libraries, agencies that illustrate America's commitment to its future, to **encourage youths to impulsively trade in the tools of aesthetics and learning for those of female exploitation and utter vulgarity**. We should gratefully embrace the opportunity that filtering devices present to prevent such tragedy. To paraphrase President Lincoln during the famous Lincoln-Douglas debates, "True liberty requires responsibility, not absolute license."

---

[24] Strossen, N. (1995). Defending Pornography: Free Speech, Sex and the Fight for Women's Rights, New York: Anchor Books, p. 161.

[25] 443 U.S. 622, 635 (1979)

COPA Commission

Information and Resources About the Commission on Online Child Protection (COPA)

Hosted by the Congressional Internet Caucus Advisory Committee

Additional Testimony for July 19-20 Hearings

The following organizations submitted written testimony to the Commission.

- Kermit Roosevelt *testimony*
- Senator Mary Landrieu (D-Louisana) *biography* *testimony*

[Home] [Final Report] [About this Site] [FAQ] [The Commission] [Press Room]
[Meetings and Hearings] [Research Papers] [Privacy Policy]

webmaster@copacommission.org / Copyright © 2000

BEST COPY AVAILABLE

Testimony of Kermit Roosevelt III

Thank you for giving me the opportunity to present this testimony. I am a fellow with Yale Law School's Information Society Project, an organization devoted to the promotion of democratic values in the information society. I received an A.B. from Harvard in 1993 and a J.D. from Yale in 1997. I have published articles in numerous law reviews and recently coauthored (with J.M. Balkin and Beth Noveck) a report on Internet filtering systems. None of this testimony should be taken to reflect the views of any of my employers.

The Internet is very large, and it is not organized territorially. These two features make it virtually impossible to control content either unilaterally (by individual end-users without the cooperation of content providers) or by legislation. Most unilateral filtering systems consist of blacklists of prohibited websites. These are invariably underinclusive; that is, they do not block all of the sites that end-users would want blocked. They tend also to be overinclusive; that is, they often block sites that end-users would not want blocked. Beyond these practical failings, unilateral filters by their nature force end-users to accept the judgment of third parties as to what is or is not acceptable. Worse still, since the value of unilateral filtering systems consists primarily in their lists of unacceptable sites, these lists are often treated as proprietary information and concealed from end-users. Thus end-users are typically denied the information necessary to decide whether a particular unilateral filter conforms to their preferences or not.

Attempts to control content via legislation face equally serious difficulties. Constitutional problems aside, legislation that affects the behavior only of content providers within the United States will tend to be ineffective, since it is just as easy to access content originating in foreign countries as it is to access American content. But legislation with an international reach is not the answer either. Whether the U.S government has the power to punish foreign website operators for failing to comply with U.S. law is far from clear as a legal matter; what is clear is that the practical difficulties are in any case overwhelming.

I believe that the only solution that has a chance of working is a multilateral one that relies on cooperation between content providers and end-users. The solution to the problem of size is to rely on content providers to label their content in a way that gives end-users the ability to screen according to criteria they select. Giving this choice to end-users likewise solves the problem of placing access decisions unreviewably in the hands of third parties, as unilateral filtering systems do.

The Information Society Project has recently written a best practices model that discusses these issues in more depth and proposes a design for a filtering system. (I am glad to see that this paper is available on the COPA Commission website.) That model relies on cooperation between content providers and end-users; it also envisions a role for third-party organizations in tailoring a generic filtering system to suit individual preferences. This system is not only more effective than legislation or unilateral filtering in practice; it is also more responsive to First Amendment concerns.

The problem that the multilateral solution faces is that it will be effective only if a sufficiently large percentage of content providers take the necessary step of rating their content. Implementation of the model filtering system is currently in the hands of ICRA, and Stephen Balkam is certainly a better source of information on how many sites are currently cooperating in the labeling project. But it is my impression that there is substantial resistance to self-labeling, due in part to a pervasive libertarian ethos. I have serious doubts as to whether this resistance can be overcome if the issue continues to be cast in terms of protecting children from material that is harmful to minors. Legislation requiring labeling of content is a superficially attractive solution, but it would certainly face constitutional challenges in the U.S. Though it is possible that the challenges would fail (labeling content may be best understood not as compelled speech but as a technological means to prevent distribution of certain content to those who, by using filtering systems, have indicated a desire not to receive it) the territorial limitations on legislative jurisdiction would likely render it ineffective in any case.

I think that the best hope for widespread acceptance of a labeling system lies in making labeling attractive to content providers. As things stand, content providers have little incentive to label (though this would change if a high percentage of end-users employed a filtering system that blocked unlabeled sites).

BEST COPY AVAILABLE

They will have an incentive to label if it brings them more traffic. And it will bring them more traffic if many or most search engines read labels.

But there will be little point in search engines reading labels if labels correspond only to undesirable content, e.g., the categories of sex, violence, and offensive language. There is unlikely to be much end-user demand for search engines specializing in that sort of content. And more significantly, with such a restricted range of labels, the vast bulk of useful websites will reap no benefit at all from labeling. If they do not label, then end-users will be forced to make large sacrifices if they want to block unrated sites.

By contrast, if labels describe a broader range of content, then search engines are likely to rely on them, and content providers will have incentives to label (and to label accurately). This is the most important point I have to make, and the point that I think current approaches to filtering miss most seriously: what makes something filterable also makes it searchable. Indeed, filtering and searching are two sides of the same coin. Content providers may not want their sites to be filterable, but they do want them to be searchable. Current search engines tend to use the presence of particular words on a web page. This gives very coarse searching; it produces the equivalent of text-based filtering systems, which are notoriously ineffective. The use of labels that describe the content of a website in a machine-readable manner will make searching much more efficient; it will also make filtering much more practical. I doubt that adoption of labeling on the scale necessary for effective filtering can be achieved by a focus on filtering; there is too much instinctive resistance and too little payoff for content providers to comply. But content providers have the opposite reaction to improved searching; they are eager to cooperate. If machine-readable labels are introduced as a means for more efficient searches, they are much more likely to catch on. But in order for that to happen, labeling must embrace a wider perspective than concern about harm to children. Broadening the focus is the best hope for widespread acceptance of labels.

BEST COPY AVAILABLE

Biography of Senator Mary Landrieu

Mary L. Landrieu became the first woman from Louisiana ever elected to the United States Senate on January 7, 1997. With her 1999 appointment to the Armed Services Committee, Landrieu also became the first Democratic woman, and only the second Louisianian, to serve on the top national security panel.

In 1979, 23-year-old Landrieu was elected to the Louisiana House of Representatives, where she served on the powerful Appropriations Committee. After two terms in the House, she served eight years as state treasurer, finding innovative solutions for the state's fiscal problems, including responsible state debt limitations and investments for education.

Landrieu is a moderate Democrat who believes our nation can and should do a better job of balancing our budget and educating our children for the global challenges ahead.

Leading for Stronger, Smarter National Security

Senator Landrieu was on the Armed Services Committee just a few months when she brokered a major compromise that broke a five-year partisan deadlock, allowing the Senate to move forward with a policy for developing a National Missile Defense system.

"During the Cold War, the United States and the Soviet Union held to the standard of mutually assured destruction," Landrieu said. "Now, we need to move toward the post Cold War axiom of mutually assured security."

Landrieu's amendment added language that made it clear the U.S. will pursue this strategy on two fronts: development and deployment of a national missile defense system to protect the nation's borders, and continued negotiations with Russia to reduce nuclear weapons arsenals.

Armed Services is an important committee for Louisiana, which houses three major military installations and is home to one of the world's largest shipbuilders. The annual economic impact of the military and defense-related contracts on the state is more than $6 billion.

A Voice For Agriculture

Senator Landrieu's appointment to Armed Services replaced her position on the Agriculture Committee. Still, she recognizes that agriculture is vital to Louisiana. While serving two years on the committee, Landrieu helped pass a $6 billion federal farm relief bill that provided more than $50 million for Louisiana farmers ravaged by drought.

Senator Landrieu is a proponent of balancing the needs of farmers with protecting the environment. She has joined a bipartisan effort to ensure the health risks of pesticides are evaluated based on sound science, protecting vital pesticides from bans that would devastate the state''s struggling agricultural sector. The Regulatory Fairness and Openness Act would give farmers access to the most effective pesticides, while protecting people from harmful chemicals.

"This legislation maintains high health standards, and at the same time, requires the EPA to make more fair and scientific evaluations of pesticides," Landrieu said.

Protecting Our Resources, Getting Our Fair Share

As a member of the Energy and Natural Resources Committee, Senator Landrieu leads a bipartisan charge to bring an estimated $300 million a year to Louisiana by redirecting a larger portion of federal off-shore oil and gas drilling revenues to coastal states. The Reinvestment and Environmental Restoration Act would represent the largest investment in the environment in decades, without additional taxes.

Since the federal government began collecting offshore oil and gas drilling revenues in 1956, it has taken in more than $120 billion, keeping nearly 100 percent. Under this bill, 50 percent would be redirected to states to preserve coastlines and wetlands. Every state would benefit from additional funding for the Land and Water Conservation Fund, the Wildlife Restoration Fund and historic preservation.

"Louisiana and other coastal states have waited too long for their fair share of offshore drilling revenues," Landrieu said. The proposed formula creates fairness for coastal states that provide invaluable natural resources to our nation's growing economy. It is a fiscally prudent plan that invests revenues from a nonrenewable resource back into renewable resources for future generations.

Advocate For Small Business

More than 65 percent of new job growth in Louisiana in the past decade was created by small businesses, making it the backbone of the state's economy. As a member of the Small Business Committee, she has helped pass legislation that has reduced federal regulations and created tax relief for small businesses. In fact, her pro-growth, pro-business voting record in the 105th Congress earned her the U.S. Chamber of Commerce's Spirit of Enterprise Award.

Building and Strengthening Our Families

Statistics on the overall health and well-being of Louisiana's children are among the worst in the nation. Thirty-two percent of children live in poverty, while more than 20 percent of teen-age girls give birth before their 18th birthday. In June 1998, Landrieu joined a number of state leaders and child advocates to launch "Steps to Success," a public/private partnership focused on ensuring all children at ready to start school. The initiative focuses on increasing learning opportunities for children from birth to age 3, the time when 90 percent of a child's brain develops.

Senator Landrieu also strongly supports an increased tax credit for families adopting special needs children. She would like to see the tax credit increased from its current $6,000 to $10,000. "Building families through adoption is a blessing for all. Children cannot raise themselves. Every child needs at least one caring adult in their life, but preferably two stable, loving parents."

Family

Senator Landrieu is married to Frank Snellings, and they have two young children. Born Nov. 23, 1955, she is the oldest of nine siblings and the daughter of former New Orleans Mayor Moon Landrieu and Verna Landrieu.

OPENING STATEMENT BEFORE 7/21/00 MEETING OF THE COPA COMMISSION IN RICHMOND, VIRGINIA

Hart Senate Office Building
Washington, D.C.
July 20, 2000

Thank You Mr. Chairman and Members of the Commission:
I want to thank you all for holding the second in this very important series of meetings here in Richmond today. Your work will provide the foundation for what I hope will be a definitive solution to the very difficult problem posed by the presence of pornography and other obscene material over the Internet. It will also eliminate the threat such materials pose to our children. Once all the data is in, I intend to offer legislation based upon the Commission's findings.

I speak to you today not only as a United States Senator, but also as mother concerned for the welfare of my children and all others. I also speak as a citizen who cherishes the protection of a strong First Amendment that is one of the proudest tenants of American democracy. In short, I find myself facing the same dilemma as most Americans: standing before the impossible (and false) choice between protecting our children from damaging, demoralizing early exposure to sexual materials and defending one of the cornerstones of our Constitution. Congress established this Commission to get all of us past this Catch 22 so we can arrive at a pragmatic, workable way to preserve the full measure of free speech for adults while allowing space for childhood. This is a high calling and today I pledge that this Commission can count on my best effort in seeking the funding and political support necessary to complete its work.

I have experienced first hand how obscene materials can enter a home and be placed unbidden before a child's eyes without adequate warning, even while a parent is in attendance and controlling the computer. One day, I was shopping online for light fixtures with my daughter in my lap. I was looking for a website called <chandeliers.com> but mistyped the web address by mistake. As a result, my search immediately pulled up a pornographic website which locked in place on my screen. I was devastated that my innocent mistake had placed such material before a child young enough to sit in my lap as I worked. I myself felt violated and misled, since the website name I typed in error was so innocuous that I had no warning of what it would produce. I felt frustrated that the Internet offered me no warning or other resource that would help me protect my daughter from exposure to such base images. This practice should not be allowed to continue and I do not believe the First Amendment will disappear down a slippery slope if we use some measured means to prevent it from happening.

Well-intentioned people on both sides of this issue can differ, and protecting either children or the Constitution can inspire polarizing rhetoric. The First Amendment can be cast as an enemy of morality and order, which is patently untrue. Perhaps even more destructive is the cynicism that suspects all arguments on behalf of children to be mere political manipulation. At its extreme, this cynicism often casts children themselves as enemies of adult liberties. In a society where child abuse is disturbingly common, we do not need a rhetoric that casts concerned parents, worse still children themselves, as hostile to free adult expression. It is time to break down the false dichotomy alarmists on both sides of this issue have created so we can work together toward solutions. I hope this Commission will be the vehicle for such cooperation.

Let me make it absolutely clear that I do not propose the wholesale banning adult materials online. People who want to see such things should have access to them. But as a parent I demand access to some means of controlling such information in my own home. Several solutions have been proposed: filtering software; an online rating system; labeling of sites within their web addresses; use of a top level domain such as "adult.com"; age verification procedures for online users; even biometric barriers, such as retinal scans. All of these have merit. No doubt some combination of these and other solutions will provide an optimal amount of control to parents without compromising the free speech rights of other citizens.

Out of genuine concern for the welfare of our children, some of my colleagues in the Senate and House have already offered legislative solutions. I salute them for these efforts, and I want to join them in addressing the clear need for Congressional action in this area. I do not feel, however, that the time is ripe for legislation until the findings of this Congressionally-created Commission have been published. When they are, I intend to work with colleagues on both sides of the aisle to arrive at the best, most workable solutions possible.

I look forward to the Commission's findings on what constitutes the best solution. Let us remember, as we await those findings, that rights untempered with responsibilities pose a threat to all our freedoms. Whether on Main Street or in cyberspace, liberty is not mere license—and all adults have a sacred moral and ethical responsibility to look out for the welfare of children.
Again, Mr. Chairman and Members of the Commission, I want to thank you for calling this very important hearing, and I look forward to the valuable record that it will produce.

COPA Commission

Information and Resources About the Commission on Online Child Protection (COPA)

Hosted by the Congressional Internet Caucus Advisory Committee

Official Hearing Notice

Request for Comments In Preparation For Third Field Hearing

ACTION: Request for submission of comments regarding the subjects to be addressed in the August hearing of the Commission on Online Child Protection.

SUMMARY: The Commission on Child Online Protection is directed by Congress to consider methods and technologies to help reduce access by minors to material that is "harmful to minors" (as defined in the Child Online Protection Act ("COPA"). As part of this review, the Commission has scheduled three public hearings to consider these methods and technologies. On August 3-4, 2000, the COPA Commission will hold its third public hearing at the San Jose State University in San Jose, California. This third hearing will cover child-protective technologies and techniques not covered at the first two hearings; how pornography is marketed on the Internet; and the likely impact of technological advances on both the delivery of information and efforts to protect children from harmful material. Today's notice seeks comments on the subjects to be addressed at that hearing.

DATES: Comments are requested by Wednesday, July 26, 2000, to permit consideration by the Commissioners in advance of the hearing. However, the record will remain open for receipt of comments until after the last hearing is completed.

ADDRESSES: Written comments should be submitted to: Kristin Hogarth Litterst, Dittus Communications Inc., 1000 Thomas Jefferson St., NW #311, Washington, D.C. 20007. If feasible, nineteen copies of the written comments should be submitted. Alternatively, the Commission will accept comments submitted to the following e-mail address: comments@copacommission.org. General submissions should be captioned: "Comments on Third Hearing Subjects."

SUPPLEMENTARY INFORMATION:

I. Introduction

The Child Online Protection Act, 47 U.S.C. 231 note, ("COPA"), as amended, established a temporary, 19-person Commission to study methods to help reduce access by minors to material that is harmful to minors on the World Wide Web. The COPA Commission is directed to submit a report to Congress, no later than October 21, 2000, on the results of this study, including:

a. a description of the available technologies and methods to reduce minorsÕ access to harmful materials (including filtering, rating, age verification systems, and others),
b. conclusions regarding such technologies and methods,
c. recommendations for legislative or administrative actions to implement the conclusions of the Commission, and
d. a description of the technologies or methods that may meet the requirements for use as affirmative defenses to liability under COPA, 47 U.S.C. ¤ 231, for unlawfully permitting minors to access harmful material.

The COPA Commission will hold 3 public hearings. On June 8-9, 2000, it held a hearing in Washington, D.C. on "one-click-away" resources, age verification systems, and creation of a top-level adult domain. On July 20-21, 2000, it will hold a hearing on filtering, labeling, and rating systems, at the University of Richmond in Richmond, Virginia. On August 3-4, 2000, it will hold a hearing on child-protective technologies and techniques not covered at the first two hearings; how pornography is marketed; and the likely impact of technological advances on both the delivery of information and efforts to protect children from harmful material. This third hearing will be held at San Jose State University, in San Jose, California.

II. Information solicited by this notice:

In connection with the third public hearing, the COPA Commission requests comments on all issues of fact, law, and policy regarding the protective technologies and techniques not addressed at the first two field hearings, marketing of pornography, and the likely impact of technological advances on the delivery of information and efforts to protect children from harmful material. The following are questions that may be considered at the August 3-4 hearing:

Additional protective technologies and techniques

1. Identify sources providing child-protective technologies not discussed at the prior hearings, including child-safe spaces on the Internet, search engines, subscription services for kids, and Internet monitoring and time-limiting tools.
2. To what extent are these technologies available and used by the public?
3. Are these technologies effective to protect children from harmful material?
4. What steps can or should be taken by business or government to increase use of these technologies?
5. Identify non-technological techniques to protect children from harmful material on the Internet, including acceptable use policies, contracts with children, and education.
6. To what extent does the public use these techniques?
7. Are these techniques effective to protect children from harmful material?
8. What steps can or should be taken by business or government to increase use of these techniques?

Globalization and the international dimension

9. How does the international nature of the Internet impact on the efforts to protect children from potentially harmful material?
10. What lessons can the Commission learn from experiences, proposed legislation or self-regulatory efforts that have been developed abroad?
11. How can the U.S. combine its efforts with initiatives around the world to make the Internet a safer place for children?
12. What effect will future U.S. legislation have on the development of efforts and initiatives abroad?
13. From an international viewpoint, what actions would you most like to see the U.S. take in this area?

Marketing of sexually explicit material

14. Identify and describe the various technologies and techniques are used to market and deliver pornographic material on the Internet, including teasers, spam, metatags, push, whisper, etc.
15. How widespread is the use of these various technologies and techniques?
16. To what extent do current child-protective technologies and techniques attempt to address the various means used to market and deliver sexually explicit material?
17. In light of the response to question 11, what additional techniques and technologies need to be developed to improve protect children from sexually explicit material on the Internet?
18. What additional steps can marketers of sexually explicit material take, to prevent delivery of that material to children?

Advances in technology and implications for protection of children

19. How will anticipated advances in technology, including convergence of the Internet and broadband, wraparound, push technologies, and other changes, affect the delivery of harmful material to children?
20. What additional child-protective technologies are being developed?
21. What efforts can or should be taken by business and government to ensure that children are protected from "harmful to minors" material despite advances in technology?

Comments filed with the COPA Commission will be made available to the public.

III. Public hearing

In an upcoming notice, the COPA Commission will make public the agenda and witness list for the August 3-4 hearing.

---

webmaster@copacommission.org / Copyright © 2000

COPA Commission

Information and Resources About the Commission on Online Child Protection (COPA)

Hosted by the Congressional Internet Caucus Advisory Committee

Guidelines for Submitting Public Comments

Since the Commission has completed its work, no more submissions can be accepted. Questions about Commission activities may be addressed to comments@copacommission.org.

[Home] [Final Report] [About this Site] [FAQ] [The Commission] [Press Room]
[Meetings and Hearings] [Research Papers] [Privacy Policy]

webmaster@copacommission.org / Copyright © 2000

BEST COPY AVAILABLE

COPA Commission

Information and Resources About the Commission on Online Child Protection (COPA)

Hosted by the Congressional Internet Caucus Advisory Committee

AGENDA AND WITNESS LIST FOR COMMISSION ON CHILD ONLINE PROTECTION (COPA) HEARING III

SAN JOSE STATE UNIVERSITY
Student Union Building
Loma Prieta Room, 3rd Floor
One Washington Square
San Jose, California
Phone: 408-924-6300

August 3-4, San Jose, California

Thursday, August 3

9:00 a.m. - 9:30 a.m. **Welcome by Chairman Don Telage and Co-Chairmen Al Ganier, John Bastian and Stephen Balkam**

9:30 a.m. - 10:00 a.m. **Introduction: Parents' Attitudes Toward the Internet**

- Robin Raskin of Family PC Magazine *biography* *testimony*

10:00 a.m. - 11:15 a.m. **Panel One: Other Existing Technologies**
Purpose: This panel will provide the Commission with information about protective technologies not evaluated at Hearings 1 or 2, including filtered search engines and ISP's, green spaces, monitoring and time limiting systems.

- Catherine Davis, Producer of Yahooligans *biography* *testimony*
- Jean Armour Polly, netmom.com *biography* *testimony*
- Dan Jude, President, Security Software Systems, Inc. *biography* *testimony*
- Kevin Blakeman, President for U.S. Operations, SurfControl *biography* *testimony*
- David Smith, CEO, Surf Monkey *biography* *testimony*

11:15 -11:30 a.m. Break

11:30 -12:30 **Panel Two: Acceptable Use Policies, Awareness Programs, and Anti-Filtering Efforts**

Purpose: This panel will describe non-technological approaches to protecting children from harmful internet material, and discuss risks associated with use of filtering and rating technologies.

- Judith Krug, American Libraries Association *biography* *testimony 1* *testimony 2*
- Nancy Willard, Director, Responsible Netizon, University of Oregon *biography* *testimony 1* *testimony 2* *testimony 3*
- Monique Nelson, COO, Enough is Enough *biography* *testimony*
- Bennett Haselton, Peacefire *biography* *testimony*

12:30 p.m. - 1:45 p.m. Lunch - Sponsored by the U.S. Postal Service

1:45 p.m. - 3:30 p.m. **Panel Three: Marketing of Sexually Explicit Material**
Purpose: This panel will provide information on how sexually explicit material is marketed, and thus allow the Commission to evaluate the extent to which the various child-protective technologies and techniques address these marketing efforts.

- Andrew Edmond, CEO, Flying Crocodile Inc. *biography* *testimony*
- Danni Ashe, Danni's Hard Drive *biography* *testimony*
- Dr. Victor Cline, University of Utah *biography* *testimony*
- Detective LeeAnn Shirey, Seattle Police Department ***biography*** *testimony*
- FBI Supervisory Special Agent Randy Aden ***biography*** *testimony*
- FBI Special Agent Bruce Applin ***biography*** *testimony*
- Detective Daryk Rowland, Huntington, CA Police Department *biography* *testimony*

3:40 p.m. - 3:45 p.m. Break

3:45 p.m. - 5:00 p.m. **Panel Four: Globalization**
Purpose: This panel will consider the legal, marketing and access issues that result from the global nature of the Internet, and will provide insight on how other countries are dealing with issues of harm to minors.

- Jan D'Arcy, Co-Director, Media Awareness Network *biography* *testimony*
- Marcel Machill, Bertlesmann Foundation *biography* *testimony*
- Barb Dooley, Executive Director, Commercial Internet Exchange Association *biography* *testimony*
- Andree Wright, Australian Broadcasting Authority *biography* *testimony* *testimony 2* *testimony 3* *presentation*
- Danny Weitzner, Technology and Society Domain Leader, World Wide Web Consortium *biography* *testimony*

5:00 p.m. - 5:15 p.m. Questions and Comments

Friday, August 4

9:00 a.m. - 9:15 a.m. **Welcoming Remarks by Chairman Don Telage and Co-Chairmen Al Ganier, John Bastian and Stephen Balkam**

9:15 a.m. - 11:30 p.m. **Panel Five: New Technology and the Future**
Purpose: The future will bring further evolution of the Internet, including more widespread use of push and wraparound technologies and the possible convergence of the Internet and broadband. This panel will permit the Commissioners to learn what changes are likely, how these changes may affect minors' access to harmful material, whether existing protective technologies and techniques will be effective in light of those changes, and the future of Internet policing

- Dr. William Tafoya, Professor of Criminal Justice at Governors State University and former FBI agent *biography* *testimony*
- Andrew Seybold, Senior Partner, Andrew Seybold Group, LLC and Editor-in-Chief, Andrew Seybold's Outlook *biography* *testimony*
- John Litten, Microsoft Corporation *biography* *testimony*
- Harris Schwartz, ICG Communications *biography* *testimony*
- Gio Wiederhold, Professor, Computer Science Department, Stanford University *biography* *testimony* *presentation* *notes*
- Mark Ishikawa, CEO, Bay TSP *biography* *testimony*
- William Clinger IV, Vice-president of Engineering, Clinger Corporation *biography* *testimony*

11:30 a.m. - 11:45 a.m. **Questions and Comments**

11:45 a.m. **Hearing adjourned**

---

webmaster@copacommission.org / Copyright © 2000

COPA Commission

Information and Resources About the
Commission on Online Child Protection (COPA)

Hosted by the Congressional Internet Caucus Advisory Committee

Additional Testimony for August 3-4 Hearings

The following organizations submitted written testimony to the Commission.

- European Commission, Directorate-General Information Society
- Nigel Williams, ChildNet
- Dr. Kimberly Young, Center for Online Addiction
- Scott Charney, Price Waterhouse Coopers

[Home] [Final Report] [About this Site] [FAQ] [The Commission] [Press Room]
[Meetings and Hearings] [Research Papers] [Privacy Policy]

webmaster@copacommission.org / Copyright © 2000

BEST COPY AVAILABLE

EUROPEAN COMMISSION
Directorate-General Information Society

Information Society Technologies: Content, Multimedia Tools and Markets
Management of information and content, including the Action Plan on illegal and harmful content on the Internet

European Union approach to illegal and harmful content on the Internet

For submission to the COPA Commission

Illegal and harmful content on the Internet

The European Commission together with the other institutions of the European Union (EU) has been active in promoting a constructive approach to illegal and harmful content on the Internet since 1996 when the Communication on illegal and harmful content[1] and the Green Paper on protection of minors and human dignity[2] were released.

Summary of the EU approach

The role of the European Commission, which has the right of initiative for legislation under the European treaties[3], has been to foster an approach which combines appropriate an non-discriminatory use of legal mechanism (what is illegal off-line is illegal on-line), industry self-regulation, user -empowerment and awareness-raising.

The Council, composed of representatives of governments of Member States, and the European Parliament, composed of the directly-elected representatives of European citizens, have both approved this approach unreservedly.

The Member States are also implementing this approach.[4]

---

[1] Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions COM(1996) 487 http://www.ispo.cec.be/legal/en/internet/communic.html

[2] Green Paper on the protection of minors and human dignity COM(1996) 483 http://www.ispo.cec.be/legal/en/internet/gpen-toc.html

[3] In the area of criminal law, the Commission right of initiative is limited and shared with Member States.

[4] As part of the PREP-ACT 4 research project, Childnet and Fleishman Hillard undertook an audit of European government-funded internet safety awareness initiatives http://www.netaware.org/gb/background/europe.htm. The European Commission has just sent a questionnaire to Member States to obtain the latest state of measures to implement the Recommendation on protection of minors and human dignity.

Bâtiment Jean Monnet, Rue Alcide de Gasperi, L-2920 Luxembourg - Office: EUFO 1266.
Telephone: direct line (+352)4301.32400, switchboard 43011. Fax: 4301.34079.

Internet: richard.swetenham@cec.eu.int

The approach can be summarised as follows:

There is a difference between illegal content and potentially harmful content.

a) illegal content

The responsibility for prosecuting and punishing those responsible for illegal content should remain with the national law-enforcement authorities, although industry and users can help by setting up and using hotlines for reporting illegal content.

Industry and users may be of assistance to the process of law enforcement, by reporting illegal content which they find and, in the case of industry, by helping to track offenders and remove illegal content from circulation. This must take place in a context of the rights and duties laid down by law and is most effective where police and industry have a regular exchange of views so that police do not have unrealistic demands on industry.

The EU Action Plan on promoting safer use of the Internet[5] provides support for setting up a European Network of hotlines, where users can make reports which may be passed on to law-enforcement and industry.

Users can also be protected against exposure to illegal content by use of technical measures and education.

b) potentially harmful content

In some countries, the law may lay down rules about certain types of content which may not be distributed to children. Harmful content includes these types of content but is wider: it is any content which a parent would prefer their child not to access on the Internet. This requires a completely different regulatory approach to illegal content, firstly because it is not illegal for such content to be distributed to adults and secondly because individual families and national cultures may have very different approaches to what is harmful.

It was not therefore thought appropriate to seek to harmonise at EU level a definition of content for which access to minors was prohibited, so existing national legislation continues to apply.

The EU does firmly support user empowerment through parental controls and education as a means whereby families can decide the criteria which they wish to apply.

The Recommendation on protection of minors and human dignity[6] supports setting up national self-regulatory systems to give more information and warnings to parents and to develop codes of conduct for ISPs and suitable rating and filtering systems. The EU Action Plan provides financial assistance for parental control technologies and awareness-raising activities.

---

[5] http://www.ispo.cec.be/iap

[6] http://europa.eu.int/comm/dg10/avpolicy/new_srv/recom_en.pdf

International co-operation

The EU recognises that international co-operation is essential in dealing with illegal and harmful content, because of the global nature of the Internet.

The following activities are already under way:

- the US National Center for Missing and Exploited Children (NCMEC) which runs the cybertipline[7], supported by the federal government, and the Australian hotline are associate members of the **INHOPE association of hotlines**, which is receiving funding from the EU for central network activities, as part of a series of contracts for the European network of hotlines of a value of over 1,500,000 euros.

- the EU is providing financial support to the **Internet Content Rating Association** (ICRA)[8], with offices in Europe and the USA and with a membership drawn from Europe, United States, Canada and Japan. ICRA's aim is to protect children from potentially harmful material while protecting the free speech rights of content providers. ICRA owns and operates the RSACi rating and filtering system.

- the European Commission held a successful meeting on safer Internet awareness in January 2000[9]. The **GetNetWise** initiative[10], which has already testified to the COPA Commission, gave a presentation of US activities in the field of awareness.

The Commission is planning to hold a large-scale international conference on safer use of the Internet in the second half of 2001. Leading players in industry, government and the voluntary sector will be invited from around the world.

---

[7] http://www.missingkids.com/

[8] http://www.icra.org/

[9] http://www.qlinks.net/iap/infoday.html

[10] http://www.getnetwise.org/

Child Safety Online

Some observations from Childnet International to the COPA Commission

The Commission has collected a huge amount of evidence from many organisations within the USA. This note provides a different perspective from Childnet International, a not for profit group based in the UK but working around the world with the mission of helping make the Internet a great place for children (see Annex 1 for a description of Childnet's functions and recent activities).

Childnet was disappointed that it was unable to accept the Commission's invitation to provide oral evidence because of scheduling conflicts. At this stage of the Commission's activities it seemed best to submit a summary of the key lessons Childnet has learned from its work. If the opportunity arose to expand on this submission through oral evidence later in the year, Childnet would be very willing to do this.

1

The Internet provides tremendous opportunities for children to discover, connect and create

In the few short years that the Internet has been widely available it has made an enormous impact on children's lives. (One testimony to this is found in the amazing quality and richness of the winners of the annual Cable and Wireless Childnet International Awards contest see www.childnet-int.org/awards)

2

The Digital Divide is a very significant issue both within the USA and around the world

There is a near universal acceptance around the world that online access is crucial for children's learning and development of essential future work skills. But the opportunity for access, at school and at home, is very unevenly spread. There are more telephone lines in Tokyo, Japan than the whole of Africa. Strategies to overcome digital exclusion (whether of poverty, isolation, physical handicap, language, ethnic group or culture) are vital to benefit the world's children.

3

The dangers children face online are real and should be neither sensationalised nor minimised

Childnet describes the main dangers as arising from issues of:

CONTENT - accessing inappropriate content including pornography, child pornography, racist/hate and violent sites.

CONTACT - being contacted through chat rooms and e-mail by those who would seek to harm or lure them.

COMMERCIAL - the blur between much content and advertising, direct marketing to children, collection of information violating privacy.

4

The USA is likely to encounter new challenges for children online sooner than elsewhere

Experience would suggest that because of its high Internet penetration the United States has tended to experience new dangers on the Internet before other countries. The debate about pornography online and its availability to children first emerged in the US in 1993/94. The issues of advertising blurring with editorial content and marketing information being collected from children were first raised by the Center for Media Education in the US in 1996. The issues of children being potentially prey to paedophiles in chat rooms were highlighted by the National Center for Missing and Exploited Children in 1997. All of these problems have subsequently been experienced in other countries.

5

Ensuring child safety online requires a comprehensive strategy – there is no "silver bullet" solution

Childnet has always argued that keeping children safe online required a strategy that would include the following elements:

- Promoting the use of great content for children (green spaces, kid's directories (eg Childnet's own Launchsite www.launchsite.org)
- User reporting of illegal child pornography and direct exploitation of children through tiplines/hotlines (see www.inhope.org for information about hotlines in different countries)
- Strong co-operative law enforcement to deal with child pornography and child exploitation online eg luring in chat rooms
- Effective internet education and awareness campaigns for parents, carers, teachers and children which are adapted to the particular audience (see Childnet's research on this subject at www.netaware.org)
- Use of filtering and other technology tools

6

Responsibility for ensuring and promoting child safety online should be shared by parents, child welfare groups, the internet industry and governments

No single sector within society has total responsibility on this issue and the most effective strategies will seek to harness the strengths of each sector. We note good examples of this approach in initiatives like the America Links Up Campaign, Getnetwise, the Internet Watch Foundation in the UK (www.iwf.org.uk), the Singapore government initiated Parental Advisory Group for the Internet (www.pagi.org.sg) and the new Australian community education body (www.netalert.net.au)

7

There needs to be a continuous investment in educating parents (carers and teachers) and children about internet skills and online safety

There has been a tendency to have bursts of activity on internet safety rather than a constant investment in reminding parents about how their children can be kept safe online. Childnet would like to see further initiatives eg when they first purchase a multi-media computer parents should receive a leaflet about how their children can have a great (and safe) time online; computers could have a pre-installed safety tips screen saver; ISPs should have a link to a resource like Getnetwise on their log on screen (not buried in the Terms of Service area).

8

No "parental control software" is 100% effective but the technical failings are often over stated

Technology tools to help parents and others prevent children from accessing unsuitable or dangerous areas online vary in their effectiveness. One recent study in the UK by the Consumers Association (a respected independent group) concluded that it was impossible to recommend a "best buy" from among filtering products because none were wholly effective. Thus it is very important not to give parents a false sense of security by suggesting a tool will avoid the need for parental involvement. On the other hand, such software can prevent many problems, and are a useful tool in an overall safety strategy, especially in places were parents cannot be present.

9

Parents are confused about filtering products and need very simple solutions which they are constantly reminded about

Childnet's focus group research on this issue in six European countries showed that parents were confused about how filtering worked and how products could be installed (see www.netaware.org) Parents wanted more information and very simple, easy to use solutions. Requiring the downloading and installation of the initial software or updates is a step too far for most parents. Constant reminders of how to make effective use of tools are necessary. Childnet commends the approach America Online has given to this issue through continual reminders about safety on its log on screens.

10

The aversion to mandatory filtering in schools and libraries is much stronger in the USA than anywhere else

There has been very little debate on this issue outside the USA. Initiatives have been taken in a number of countries with strong public support. In the UK, the government encourages the use of filtering in schools and has approved certain approaches (see http://managedservices.ngfl.gov.uk/); in Singapore, Internet Service providers have to offer customers the option of a "Family Access Network" with filtering at the ISP's server (see www.sba.gov.sg)) ; and Australia's new legislation requires ISPs to offer filtering products to customers.

11 The effort to build an internationally acceptable not for profit labelling and filtering architecture should be supported

The issue of safety online is so important that new approaches must be investigated and supported. The initiative of the Internet Content Rating Association (www.icra.org) is one such approach that is very attractive as it does not rely on blocking software keeping up to date with new and dangerous sites. It also has the potential to include green lists of good sites for kids, to allow third party groups to add value to the system with their own templates of what content might be acceptable and from the outset has focussed on building a globally acceptable approach. Childnet supports this not for profit effort

12 The USA has a crucial leadership role in child safety online issues but can learn from some approaches developed in other countries

Childnet applauds the continuing priority being given in the USA to finding effective online safety solutions for children. As noted in point 4 above, the USA has experienced many problems earlier than elsewhere, and has thus experimented with many of the possible solutions before other countries. Thus the findings of the COPA Commission have a global as well as a national significance.

However, there are some interesting initiatives being taken in other countries from which the USA might benefit eg the commitment to internet education and awareness in Singapore (eg see the number of government supported seminars for parents on the home page of www.pagi.org.sg); the controlled use of filtering technologies in schools and libraries in the UK; the internet industry support for tiplines/hotlines in Europe.

Nigel Williams
Director
Childnet International
nigel@childnet-int.org
www.childnet-int.org

Annex 1 - Functions and Activities of Childnet International

FUNCTION AREA	EXAMPLE OF PROJECT OR ACTIVITY
Access - promoting broad access to the internet by children and highlighting quality content	Cable & Wireless Childnet Awards - an annual contest opento children from around the world and thoseworking with them engagedin innovative activities online. In April 2001 the ceremony will be held in Washington DC www.childnet-int.org/awards Launchsite an online directory of web sites offering safe and fun activities in which children can getinvolved www.launchsite.org Deafchild International - Childnet provided support to an existing deaf children's organisation to create a new initiative linking deaf children through the Internet www.deafchild.org
Awareness - helping parents and other adults supervising children be aware of the opportunities and dangers online .	Research Project for European Commission - in January 2000 Childnet submitted a report following a year long research study (undertaken in partnership with Fleishman Hillard) into how to communicate safe use of the Internet to parents and children www.netaware.org Net Benefit seminars - In 1998 Childnet helped prepare the curriculum for the America Links Up campaign in the US. Later we developedour materials into a seminar for parents and produced teaching notesfor trainers. These materials have now been usedin a number of countries including Singapore and Austraila
Protection - strategic international initiatives to directly protect children from exploitation online	INHOPE - Childnet has worked to gethotlines or tiplines inside and outside Europe, that receive reports about child pornography online, to cooperate.We established the Internet Hotline Providers in Europe Forum in 1998 and this has now becomean association - www.inhope.org International Conference on Combatting Child Pornograpy on the Internet - Childnet was invited by the US Department of Justice, the European Commission and the Austrian Government to help organise this ground breaking conference in Vienna in October 1999. www.stop-childpornog.at
Policy - engaging in strategic discussions on how access, awareness	Bertelsmann Foundation Experts Group - Nigel Williams director of Childnet served as a member of this international forum which contributed to the Bertelsmann Initiative on Self-Regulation of the Internet www.bertelsmann-stiftung.de/internetcontent Internet Content Rating Association - Nigel

and protection policies that help children can be developed and implemented	Williams served as a member of the Advisory Board to ICRA commenting on the development of this new labelling and filtering architecture for internet content. Nigel was elected to chair the Board and prepared the first draft of its report www.icra.org

Testimony of Dr. Kimberly S. Young for COPA Commission

Executive Director
Center for Online Addiction
Bradford, PA
http://www.netaddiction.com

August 3, 2000

BACKGROUND

Dr. Kimberly Young is a licensed psychologist and founder of the Center for On-Line Addiction. Dr. Young is also an Assistant Professor of Psychology at the University of Pittsburgh, Bradford, and a member of the American Psychological Association, the Employee Assistance Professionals Association, the National Council for Sexual Addiction and Compulsivity, and a founding member of the International Society of Mental Health On-line. Dr. Young serves on the editorial board of *CyberPsychology and Behavior*, is the editor of the *CyberHealth E-Newsletter*, and serves on the advisory board for Addictionsolutions.com and the Web Development Task Force at the University of Pittsburgh, Bradford. She recently served as the National Spokesperson for Reuters International, Inc., regarding their study on Information Addiction Worldwide.

Dr. Young travels both domestically and abroad to conduct workshops on the treatment of cyber-related disorders and the development of comprehensive web-based treatment programs for healthcare organizations (e.g., Support Group Management, Aftercare Programs, Staff Training, and Supervision). She has testified in both state and federal courts regarding her pioneer research and recently authored *Caught in the Net*, the first recovery book for Internet Addiction, already translated in four languages, and she is a frequent speaker on how technology impacts human behavior. She has published numerous research articles on familial and social impact of the Internet and her work has been widely covered in the media including major articles in The New York Times, USA Today, TIME, Newsweek, and the Wall Street Journal. Dr. Young is also a frequent commentator for radio and television including ABC World News Tonight, Good Morning America, Fox News on Health, and CNBC Market Watch.

The Center for Online Addiction was founded in 1995, and is considered the first training institute and behavioral healthcare firm to specialize in Internet-related conditions such as problem day trading, compulsive online shopping and gambling, cyberaffairs and infidelity online, cybersexual addiction, and the social dangers of computing on children. The firm conducts diagnostic and forensic evaluations for criminal and domestic legal cases, provides outpatient clinical services to individuals and families, and conducts healthcare workshops. In conjunction with the Bradford Area School System, the Center is currently producing two educational videos for parents and educators concerning Internet use and abuse among children and adolescents. The Center for Online Addiction is internationally recognized as a leading healthcare research firm and regularly consults with corporate and government agencies. Netaddiction.com serves the firm's web-based resource network and offers consumers the most comprehensive educational resources on e-behavior including a bibliography of references, a bookstore, message boards, research articles, referral links, an array of self-tests, and a monthly e-newsletter.

HOW THE INTERNET DIFFERS FROM TELEVISION AND WHY WE SHOULD BE AFRAID

Thank you for inviting me to speak with you today. I have been asked to provide testimony regarding the psychological ramifications of online sexually explicit material on children and adolescents. With the advance of technology, we have created a medium that far surpasses the role of television in our lives to create something that has revolutionized the way we conduct business and communicate. We have encouraged children and adolescents at younger and younger ages to use this new technology. Computer makers have now launched entire computer systems and software designed for toddlers, who will surely learn how to use the computer long before they learn how to read. And we now have a young digital generation where the Internet has become an integral part of their daily lives. At a recent lecture I presented to the Arkansas Governor's School for the Gifted and Talented, I saw how immersed teenagers had become with the Internet. The mere mention of "Internet Addiction" and all its associated societal problems made them feel as if I had launched a personal attack on their lives. As one young male put it, "The Internet is my life, so by calling the Internet bad, that is like calling me bad."

We initially encouraged children to view television with the same zeal, as we believed that television would offer vast educational benefits for children, only to realize much later that we were wrong. With decades of research, studies have documented the negative impact of entertainment television viewing in terms of intellectual and social abilities, and its potential to influence violent behavior among children. And the American Academy of Pediatricians has recently announced a ban on television viewing among children under the age of two years. By the same token, while we have encouraged young people to utilize information technologies, we have subsequently come to realize several severe and dangerous disadvantages especially towards children and adolescents.

As I present my testimony on how the Internet differs from like television and why we should be afraid, I do not mean to be an alarmist. Nor, in any way, do I mean to minimize the positive educational qualities the Internet has to offer. I am merely trying to a pragmatist and a realist as we search for the best answers that will benefit the future well being of our children, and I submit my observations to the commission in the hope that it will assist you in developing positive, effective remedies and solutions.

PSYCHOLOGICAL RISKS TO CHILDREN

Even without decades of research, we have already come to understand the significant dangers that lurk in cyberspace for children such as cyber-predators and the inadvertent exposure to pornographic images. In the following passages, I profile the psychological impact these dangers have upon children and adolescents. Integrated with this discussion, I will highlight instances of how television differs from the Internet and the role cyberspace plays in the development of these risks.

A. Unwanted Pornography in an Unregulated Society

Television stations and cable channels are owned and operated by an entity, typically a corporation like Time-Warner, Disney, or General Electric who must comply with governing bodies, such as the Federal Communications Commission. By comparison, the Internet is a global communication medium not owned by any one person, company, or country. As such, the Internet is therefore uniquely positioned as the first completely unregulated entity and uncensored communication and information device. So then how do we regulate an unregulated society? In my view, this is perhaps the toughest obstacle we face today as we contemplate how to remedy the situation under discussion today.

1. Transmission of Illegal Pornography

Reports from industry analysts support that adult entertainment is the largest online industry. Online pornography, more commonly known as Cyberporn, is so abundant and intrusive that innocent keyword searches can lead to pornographic material. The range of pornography varies from centerfold *Playboy* types of images to graphic, obscene, and possibly illegal material, turning words such as "young" "teen" "child" or "boy" into trigger words to find indecent online pornography. For example, a friend of mine who happens to be a priest wanted to learn how to surf the Internet. We logged on to my home computer and he typed in my name, Kimberly Young, as a keyword search. My web site came up and two other related sites followed. Much to our surprise, and to my embarrassment, there were several adult web sites that were found such as "Kimberly's Penthouse" "Kimberly's Playmates" and "Young Teen Pics". Cyberspace, with its lack of restrictions, is laden with hard-core porn, banned in many parts of the world, such as child pornography, and with a click of button may be transmitted across continents.

2. *Aggressive Marketing Tactics*

Sexual online content is not only abundant, but the industry utilizes aggressive marketing tactics designed to reach unsuspecting e-consumers. Marketers deliver unsolicited email advertisements to users to encourage adult viewing and cleverly disguise pornographic web sites in hopes of generating new business from accidental searches. For example, one pornographer registered the URL *Whitehouse.com* so when unsuspecting users search for the White House's official web site (*Whitehouse.gov*), they will mistakenly reach a porn site.

To exacerbate the problem, the major porn providers (it's believed that four huge operations control about 80% of all the porn sites) have all implemented newer Hypertext Markup Language code on their pages that does not allow a user to exit the site, more commonly known as "mouse jacking". New pages are loaded when you either try to exit the page or go backwards with the reverse arrow, making it easy to get stuck in one of these endless porn loops.

These sites show lewd and graphic pictures on their opening screens, making it especially troublesome when children stumbles onto one of these sites.

3. Children Intentionally View Online Pornography

While much of the concern has focused children who accidentally bump into pornographic web sites, there is a growing concern among those who go in search of such material. Unlike computer use, television use involves listening to televised programs. While some web sites utilize audio and streaming video, making the Internet more television-like, the majority of users surf through readable content, making the Internet experience quiet with the exception of keyboard typing noise. Without the availability of sound, parents are unable to overhear what children are doing on the Internet.

While many parents utilize parental filtering software, computer-literate teenagers can easily dismantle this software. In fact, several web sites are available that show teenagers how to get around monitoring and filtering software. In other instances, parents mistakenly trust their children not to view sexual material online or are completely unaware of how accessible it actually is. For example, I met one teenaged-male who downloaded nearly 8,000 pornographic images from the Internet. When I asked about his parents, he explained that they both worked full time and left him home alone with his own computer and telephone line.

Additionally, through the invention of the Internet, the adult entertainment industry has found another distribution source for adult movies through the application of streaming video that online users can download. Therefore, not only should we fear how easy it is for children to access pornographic still images but we should also consider their access to X-rated moving pictures and video from the Internet.

B. Interactivity and its Impact on Children

Television viewing is a one-way, passive communication medium. A simple-point-and-click of the remote will guide a viewer through various televised programs. In comparison, the Internet is an interactive two-way electronic medium. A person must type messages in a chat room to meet virtual partners, to read or write a post in newsgroup, to search out web sites, or to scan streaming video online. We can exchange ideas and thoughts via interactive chat rooms. While this is one healthy use of the technology, more often than not, these chat rooms contain sexually explicit dialogue, even in non-sexual chat rooms.

A chat channel is a virtual community designated with a specific name where people with common interests can get together to exchange ideas or files. The theme of the room is designated by its name, and many Internet Service Providers (ISPs) permit sexually oriented chat channels to exist with names that clearly indicate the types of sexual practices which will be "discussed" by the participants. Those practices range from the most ordinary to the most deviant.

People communicate with each other in chat channels in real-time by typing messages to each other. These messages can either appear in the public forum for the entire room to read or an "instant message" that can be sent privately to a single member of the room. I have observed that people can engage in erotic dialogue with each other, commonly known as "cybersex". That is, two or more users can co-create a sexual fantasy together, typically tailored to each one's desires, and the act may be accompanied by sexual self-stimulation. Most often, the assumption for what is mutually desired is taken from the chat room where the "cyberlovers" meet online such as "Married and Cheating," "SubMan4Female," "Fetish Fantasies" or "Bisex Fun." Names of chat rooms may also include highly deviant and repulsive themes such as, "Daddy4daughter" "Men for Barely Legal Girls" and "Incest Room".

To facilitate the experience and meet others, online subscribers invent screen names or handles that permit them to participate anonymously within all online activities. With respect to sexually explicit chat rooms, it is not uncommon to find handles such as "MarriedM4Affair," "Kinkygirl," or "SubM4F". Online users may go by several different handles changing their online persona according to their moods and desires. For instance, a 51-year-old corporate executive can go by the handle "College Stud" and pretend to be a young college football player, or "lovetoy" and pretend to be a thirty-year-old woman. In this manner, it is unclear who you are really speaking with in a chat room. It is unclear if a user is talking with a twenty-year-old female or a fifty-year-old male. The availability of anonymous, interactive, fantasy role-play chat rooms leads to the following implications for children.

1. Online Victimization

Sexual offenses against children constitute a significant proportion of all reported criminal sex acts. Rather than playgrounds and schoolyards, cyberspace now provides an easy breeding ground for child sex offenders to engage and meet children. Pedophilia and paraphilia are the most common classifications with respect to sex crimes involving the Internet. Pedophilia involves sexual activity with a prepubescent child (generally age 13 year or younger). Pedophiles online demonstrate a past history of sexual conduct with children and transfer this sexual interest to cyberspace. This generally involves producing illegal images to trade online (i.e., child pornography) or making contact directly with children through chat rooms. Paraphilia involves recurrent, intense sexually arousing fantasies, sexual urges, or behaviors generally involving 1) nonhuman objects, 2) the suffering or humiliation of oneself or one's partner, or 3) children or other non-consenting persons that occur over a period of at least 6 months. A paraphile demonstrates a predilection for arousing fantasies that he or she can now sexually act out through fantasy role-play chat rooms that cater to that particular sexual urge (e.g., bondage, rape, or incest).

The Grunwald Associates, a California marketing firm, found that there are now 25 million 2- to 17-year olds on the Web, up from 8 million since 1997. By the year 2005, the number of children online is expected to increase by another 70 percent, the survey projected. According to Peter Grunwald, president of the firm, children were found to be the primary reason behind household decisions to purchase a computer and gain Internet access. Another study conducted by the Crimes Against Children Research Center at the University of New Hampshire found the following statistics related to online victimization:

- 1 In 4 Children Who've Gone Online Have Been Solicited
- 1 In 5 Has Been Sent Provocative Pics Thru Web Contact
- 725,000 Have Been Asked To Meet For Sexual Purposes

Studies repeatedly show that the Internet is not a safe place for children, and extra precautions such as careful parental monitoring and the implementation of filtering software should be taken before children should be allowed online.

2. Teen Sexual Experimentation

Television is seen as social activity as we can watch our favorite sit-coms, the evening news, or the latest movie on HBO together with family and friends. In comparison, using the computer is generally seen as a solitary activity, with smaller viewing screens than television and a single keyboard unit. With the advent of Internet-enabled devices such as the Palm Series, the Internet is becoming increasingly more personalized and solitary. At an alarming rate, children are still left unsupervised at the computer.

Children who are unattended can easily enter these chat rooms. One suspicious mother used a pair of binoculars through an open window to spy on her fifteen-year-old daughter only to discover she was having cybersex with men who were in their thirties and forties. Another mother discovered her sixteen-year-son had corresponded with thirty-eight different women online, all over the age of eighteen. Worse yet, we hear horror story after horror story of teenagers who run off with people they met over the Internet.

New technological advances create a new set of problems that make it increasingly difficult to protect children. Beyond the scope of our discussion involving interactive chat rooms, live web cam sex is an increasingly popular form of online sexual behavior. That is, the use of video cameras that allow two (or more) users to simultaneously broadcast to one another via the web to view faces or body parts, while typing messages or talking on the phone or through a voice chat system. It is not uncommon for children to interact with friends, meeting new people, and sexually experiment through web cams, opening up even more opportunities for cyber-pedophiles to reach children.

3. A Community for Pedophiles

Television broadcasts are limited in scope by the number of channel selections available via cable networks and the range of viewer programming. Television stations pre-determine broadcast sequence and time slots. In comparison, the Internet is an infinite loop of information, news, chat rooms, discussion groups, and content that collectively provides a continuous stream of changing, evolving, interactive stimulation. With over an estimated 3 billion web sites, each Internet session can be a unique experience customized to your specific interests. Plus, unlike television, the Internet affords users the opportunity to *create* new dynamic content. The uncensored nature of cyberspace coupled with its seeming anonymity provides child pornographers with a new medium to pursue potential contacts and clients (both in terms of children and fellow pornographers). Child pornographers will not only create their own web sites but frequently *spam* (send child porn pictures to multiple and random online users) in hopes of finding others who share their interests to trade pictures and secrets about ways to meet children.

4. The Growing Prevalence of Travelers

There is a sharp rise in the number of sexual predators who prowl the Internet looking for vulnerable children, and who then make arrangements to meet the child for sex. The FBI calls these criminals - "travelers". The numbers are hard to document, but travelers are clearly part of the Internet-era crime way. According to a recent CBS News report, the FBI alone opens up six new traveler investigations every week. The Center for Missing and Exploited Children receives about 15 new leads about online enticements each week. A traveler is arrested somewhere in the United States almost every day. The profile of the traveler is that of a first-time offender with no previous history of criminal activity or psychiatric illness. Some noted examples are Patrick

Naughton of Infoseek/Go.com, Terry Spontarelli, a Los Alamos research chemist, George DeBier, a former Belgian diplomat, William Bowles, former CEO of iBeam.com.

How does cyberspace serve to encourage this type of behavior from otherwise pro-social and law-abiding citizens? Are these just pedophiles in disguise or does cyberspace serve as an enabler for sexually deviant behavior to develop? My contention is that the Internet's sexually graphic, uncensored, and interactive online culture serves to encourage and validate such sexual acting out online. This explanation is not intended to rationalize or excuse this type of behavior, but rather to understand how cyberspace contributes to its development and growing pervasiveness.

First, the proliferation of sexually explicit chat rooms, groups, and games contributes to easy access for a curious person's initial exploration. Most people do not yet realize that there is any risk involved in engaging in online sexual pursuits. While in some ways it may seem like a journey into "foreign territory," online sexual behaviors occur in the familiar and comfortable environment of home or office thus reducing the feeling of risk and allowing even more adventurous behaviors.

The anonymity associated with electronic communication, and the general milieu of the Internet often facilitates more open and frank communication with other users. Within the anonymous context of cyberspace, conventional messages about sex are eliminated allowing users to play out hidden or repressed sexual fantasies in a private virtual lab. This leaves curious individuals the opportunity to sexually experiment online and these fantasies may progress gradually into darker and darker themes that in real life, they would normally find reprehensible only to become increasingly acceptable online. Among incest-theme chat rooms, users typically participate with others who take on character roles and *pretend* to be younger. With repeated exposure, users may become desensitized to the experience and this may possibly reinforce future real-life actions such as traveling. More often, in my experience, these 'fantasy' users engage in virtual role-plays without the intention of making direct contact with children. However, the potential *creation* of travelers via cyberspace increases the risk to children's safety as well as raises legal questions about the role of Internet-enabled pathology in the development of online criminal conduct and its ramifications on rehabilitation efforts and sentencing judgments.

IN CONCLUSION

Due to its lack of restriction and interactive nature, we can see that the Internet has more far-reaching implications than television ever had in children's lives. We have struggled to find fair and equitable remedies to a complex problem. Hopefully, technology itself will be able to provide some of the solution by creating individualized Internet channels that separate pornographic and other unsuitable material for children. However, the main points presented here clearly indicate that the problem goes beyond regulation of "Internet smut" as the interactive capabilities pose an equal, if not more dangerous threat to the welfare of children.

In the future, with computer technologies becoming increasingly more personalized through Internet-enabled devices, monitoring children will pose an even greater challenge to parents and families. Some general solutions that we at the Center for Online Addiction have developed include:

1) Incorporate comprehensive child and parent Internet safety educational programs throughout K-12 school systems designed to aid in prevention of child victimization.
2) Develop media campaigns akin to public announcements such as "Don't Drink and Drive" to raise public awareness of the social dangers of cyberspace.
3) Launch "E-User Education Programs" to promote responsible online usage and computing behavior among adults.
4) Enlist the help of Internet Service Providers themselves in the close supervision of inappropriate online conduct, especially among crimes against children.

Together I hope we can find ways to harness the Internet's positive potential while making it safer place for children as well as adults.

PRICEWATERHOUSECOOPERS

Memo

To: The COPA Commission

From: Scott Charney

Date: August 28, 2000

Subject: COPA Commission Comments

First, I would like to apologize for being unable to attend the Commission's recent hearings in California, and thank the Commission for its willingness to accept written comments. Your specific tasking -- which includes finding ways of reducing minors' access to material that is harmful to them on the Internet -- is indeed a daunting one, both legally and technically.

Legally, efforts to protect minors using the Internet have yet to survive constitutional challenge. Key provisions of the Communications Decency Act and Child Online Protection Act were struck down, the latter after serious attempts to address the flaws of the former. Most striking is the Third Circuit's conclusion that: "[W]e are forced to recognize that, at present, due to technological limitations, there may be no other means by which harmful material on the Web may be constitutionally restricted, although, in light of rapidly developing technological advances, what may now be impossible to regulate constitutionally may, in the not-too-distant future, become feasible." The subtext of this statement is that we have allowed technology in general, and markets in particular, to dictate public policy, and now must live with that decision.

Technically, efforts to protect children have also been limited in effectiveness. URL-naming conventions (such as a top level domain of ".kids") or other identifiers do not currently exist. Additionally, content filtering has inherent limitations at both ends of the spectrum: they risk being underinclusive (giving children access to inappropriate material) and overbroad (denying children access to material that is actually appropriate).

It is against this backdrop that I do have one suggestion: the Commission may wish to consider recommending to Congress the enactment of legislation which prohibits mislabeling website content as being suitable for children.[1] Significantly, the legislation should not require a website to be labeled; it should only provide that if a label is applied, it must be truthful. (Compelled labeling may violate the First Amendment, as it might constitute compelled speech.)

This legislation would enable market based products to function more effectively. More specifically, parents could demand and deploy filters that affirmatively look for a child-friendly label, prohibiting their children access to those sites that are either unlabeled, or not specifically labeled as safe for children. In response, those seeking to attract children would tag their websites as "child friendly," and falsely doing so would result in penalties. As for the penalties themselves, there are of course several options. One approach might be to provide for injunctive relief, as well as a civil penalty, in the case of a mislabeled site, with stiffer sanctions -- perhaps even criminal penalties -- if it could be proven that an individual/organization intentionally mislabeled a site.

---

[1] This idea was suggested to me by Philip Reitinger, Deputy Chief of the Computer Crime and Intellectual Property Section at the U.S. Department of Justice. I mention this so as to not receive undue credit for the idea, but I also do not wish to imply that this approach has been approved or adopted by the Justice Department.

COPA Commission

Information and Resources About the Commission on Online Child Protection (COPA)

Hosted by the Congressional Internet Caucus Advisory Committee

The Commission | Press Room | Meetings · Hearings | Research Papers | About this Site | www.copacommission.org

Research Papers

Y. Akdeniz	The Governance of Internet Content Regulation in Europe The Regulation of Internet Content in Europe: Governmental Control vs. Self-Responsibility
David Burt	Dangerous Access, 2000 Ed: Uncovering Internet Porn in America's Libraries [.pdf]
European Union	The Recommendation on Protection of Minors and Human Dignity [.pdf] The Action Plan on promoting safer use of the Internet [.pdf]
Gay & Lesbian Alliance Against Defamation	Access Denied, Version 1.0: The Impact of Internet Filtering Software on the Lesbian and Gay Community [.pdf] Access Denied, Version 2.0: The Continuing Threat Against Internet Access and Privacy and Its Impact on the Lesbian, Gay, Bisexual and Transgender Community [.pdf] Access Denied, Version 1.0: The Impact of Internet Filtering Software on the Lesbian and Gay Community [.pdf]
Greenville South Carolina Library Board	Internet Use Policy [.pdf] Report [.pdf]
Christopher D. Hunter	Cyberporn, Filters, and Public Policy: A Content Analysis Research Proposal [.pdf] **(with Eric A. Zimmer)** Risk and the Internet: Perception and Reality Internet Filter Effectiveness: Testing Over and Underinclusive Blocking Decisions of Four Popular Filters [.pdf] Filtering the Future?: Software Filters, Porn, Pics, and the Internet Content Conundrum [.pdf]
Information Society Project at Yale Law School	Filtering the Internet: A Best Practices Model
Lawrence Lessig	G-Rated Browsers What Things Regulate Speech: CDA 2.0 vs. Filtering [.pdf] The Tyranny in the Infrastructure

BEST COPY AVAILABLE

	(with Paul Resnick)Zoning Speech on the Internet: A Legal and Technical Model [.pdf]
Markkula Center	Access, Internet, and Public Libraries: A report to the Santa Clara County Libraries
Morality in Media	Comments of Morality in Media, Inc. [.pdf]
Crimes against Children Research Center/ National Center for Missing and Exploited Children	Online Victimization: A Report on the Nation's Youth [.pdf]
OCLC Office of Research:	Web Characterization Project: Statistics
Peacefire.org	Project Bait and Switch First Report on Exotrope's BAIR blocking program Second Report on Exotrope's BAIR blocking program Report on Clicksafe's blocking program Sites blocked by FamilyClick Sites blocked by Cyber Sentinel SurfWatch error rate for the first 1,000 .com domains on the Internet
Crystal Roberts, Family Research Council	Filtering and Blocking Technology: The Most Effective Methods of Protecting Children from Internet Pornography
Richard S. Rosenberg	Controlling Access to the Internet: The Role of Filtering [.pdf]
U.S. National Commission on Libraries and Science	Kids and the Internet: The Promise and the Perils [.pdf] Moving Toward More Effective Public Internet Access [.pdf]
Jonathan Weinberg	Rating The Net

[Home] [Final Report] [About this Site] [FAQ] [The Commission] [Press Room]
[Meetings and Hearings] [Research Papers] [Privacy Policy]

webmaster@copacommission.org / Copyright © 2000

BEST COPY AVAILABLE

Comments to the COPA Commission

I have a question regarding the use of pornography on the Internet. Pornography is something that will not be stopped no matter how hard people try to stop it. I know that COPA has been tasked with making recommendations to congress on how to reduce the chance of minors accessing pornography.

I have dealt with this for some time while working for an Internet service provider. I would get phone calls every day with questions and comments about how to stop adult content from being seen by children. The company I used employed a product called X-Stop, which worked well but there would often be times that it would still let some stuff through. One saying that I remember well is if you build something idiot-proof someone will build a better idiot. That has been seen time and time again. If some sort of technology was implemented it would only be a matter of time before that technology has been broken. My suggestion is to make things easier, is restrict adult content sites to something with a domain of .xxx or something like that. When adult sites are allowed to make use of a .com or a .net or a .org that only makes it easier for children to view adult content and it also allows search engines to display such results because of misleading descriptions of sites. A simple search for dollhouse on any major search engine will bring up more adult sites than actual sites on dollhouses. The same goes for any searches for any famous star such as Britney Spears, Backstreet Boys, and Julia Roberts. More and more sites are going online everyday and they may a killing with the use of banner ads and misleading search descriptions. I think it could be easily avoided if adult sites were restricted to the domains of .xxx. That would not infringe on the rights of those who like to publish that sort of content. In fact it allows it and gives them their own place on the Internet. Cities and towns across the world using zoning rules for residential, industrial, and commercial zones of where company buildings can be built, why not recommend to the domain registration sites that rules of that sort be enforced. If it were legal in the US, then the government could levy fines against the web site operators, or web hosting companies that allow someone to post a adult content site in any area other than a .xxx domain, and to apply that with the use of redirection. Where someone would put a page on a good domain that automatically redirects the surfer to a .xxx page.

These are just my ideas on how to help the online community.

Sincerely yours,

Tee Jay Harrison

You know, if the Commission would analyze the business model of the "Porn" industry, it would be far more successful than the content based approach and the First Amendment issues it raises.

There are 2 points regarding "Porn" and the Internet which the Commission should consider:

First, the Internet will severely dilute earnings for adult image production. Images from all major adult hard copy magazines are available for free on the Net before the magazines even hit the newsstand or very soon thereafter. Ultimately, this will cut into subscription, retail sales, and production of adult material. There appears to be no way to stop the free flow of these images over the Net. This flow of images includes adult movies. The technology to "digitize" and make available on the Net adult images is very inexpensive. At some point the adult industry will feel the monetary loss. When this happens, the industry will attempt to use copyright laws to protect their business.

This is where the second point comes into play. While content and protection of minor laws might still be pursued, copyright laws could be more easily modified to accomplish the same ends. It is a supply rather than a demand approach. The copyright laws could be changed to allow that any adult material intentionally or recklessly or negligently made available to minors would automatically cause a complete loss of any copyrights and make the material public domain at the moment of the offense. This would extend to any licensee or vendor of the material, or any provider in the retail revenue stream. Public policy and protection of minors should have a far greater weight in a copyright analysis than a First Amendment analysis, remembering that this is a novel approach. This would evolve into a equal protection claim based on the copyright standard of scientific and useful arts - a dead on arrival and laughable claim for the adult image industry, but would also leave untouched educational or medical material. Every copyright claim by adult image producers/rights holder would have the specter of an availability to minors infraction hanging over its head. The industry is now forced to either self police the dissemination of the material or lose all copyrights in the material. The copyright modification will also impact even the smallest producer of adult material. This would also provide very high ground in the public relations/ public policy arena. It boils down to thus- while you may have a First Amendment right to produce this material, by making it available to minors you lose your rights to availing public resources to protect copyrights for the material.

In the final analysis, the question becomes- who will produce and disseminate adult material under this proposal without self imposed strict guidelines on its dissemination ? The copyright modification will also have an impact on foreign sources. If the United States will not enforce their copyright claims in the American market, they must avoid the U.S. markets or risk losing rights to their property. While most attention is being applied to the Net and copyright enforcement, it seems no one is thinking about the Net and loss of copyright protection.

Best Regards
R Allen

I was reading this morning's news and noticed Mr. Telage's comments regarding our needing to get "more bang for the buck" with respect to the goals of curtailing the distribution of materials harmful to youngsters. I could not agree more!

So much misplaced anger and non-productive effort is being spent on bravado and silly enforcement schemes when, as Mr. Telage correctly observes, the secret is in education, not in enforcement. If you will forgive me an analogy:

In the early 1950s, people regularly threw their food containers, Kleenex, pop bottles, and beer cans from their car windows as they drove down our streets and highways. California instituted a $5,000 fine and a 6-month prison term enforcement threat, which it posted on nearly every major street, highway, and biway. Even as a child, I found that to be a silly waste of money. In fact, I never heard of anyone ever being fined anything approaching $5,000 or anyone ever going to jail for a week under the law, let alone 6 months! However, state funds were also allocated toward fashioning a well organized education campaign which helped people realize that they didn't want to live in each other's collective garbage cans. Now we just about never see anyone throwing anything larger than a cigarette butt from their car window. The signs have mostly disappeared; the penalties are still on the books, but it was the educative process that corrected the problem.

So, I applaud Mr. Telage and his wisdom in this matter.

Ken Tennen

The problem of children inadvertently accessing pornography on the Internet could be greatly reduced by designating all sex sites to broadcast under particular domain name, for instance the web extension, [dot]sex. Any address with that extension would indicate a site that could contain sexually explicit material. This would essentially create a sex channel on the net. People who want that content can access the channel, people who don't want the content, and set their Browser to block any such addresses with that extension from loading.

Then browsers would have no problem filtering the data, and anyone who wants to see it, can access it easily.

This is the best type of regulation, it is not a restriction on doing business, but a definition of the playing field designated for that business. It does not block sexual expression, it just regulates it to a specific marketplace.

Regulating sex sites to a specific channel, would provide consumers with a powerful level of control that they currently do not possess. Violations, whether foreign or domestic would be easy to detect, and enforcement centers on whether the content was sexually explicit or not, rather than on free speech issues, a considerably simpler issue for the courts to handle. Violators should be subject to significant fines .[I would suggest fines be based on a percentage of annual revenues, rather than fixed amounts.]

The real issue for society is whether consumers can control what content comes through their browser. The government has a role to play in providing that protection. This type of regulation does not seek control over what is broadcast, that is free speech, it seeks to establish controls over what is received, and allows consumers to implemented that control on an individual basis.

This solution would be a low cost and relatively easily to implement.

That's my 2-cents.

Thanks
Stephen Kennedy

I just saw you article Anti-porn Group To Suggest Online Children's Section on CNET news (news.com). I think you are missing one basic point. We should not have to create a save section for the kids on the Internet, we just need you create an adult section on the Internet. Just like the adult area of town that you can find in most middle to large size city

Think of it like this, you have your neighborhood bookstore the one that everyone can enter and then you have the adult bookstore where you have to be of a curtain age to enter. By setting up the Internet in this fashion you have solved both the privacy and free speech concerns.

One other thing you need to do if you create an adult section, on the Internet then you need to require all search engine to add a section the asked the ask what type of site would you like to search (com, gov, est. or xxx). This way you should not have to worry about the freedom of speech, because if someone wants to go to XXX all they have to do is to check that box.

Well I got to go now I hope this helps.
Bob Callegari

I don't know whom to address this question to, nor do I know what impact my suggestion may have or if it has already been thought of. However, the need for control of adult sites really needs to be managed and monitored to a stricter level. The technologies out right now trying to prohibit children or users from accessing adult content sites is simply not working. Even the login screens for many of the sites are very seductive. I don't think I have to preach to this commission in regards to this matter.

My suggestion is quite simple in explanation. However it may be more difficult to approve and execute. For all sites containing adult matter, there should be an ".adu" extension. There is already tight control on the use of ".gov" or ".us" extensions. Why can there not be a mandatory ".adu" extension for all adult related sites. This way you could have an option in the securities of the browser to not allow access to any ".adu" URLs. I will be very happy to assist in creating a requirements document or help in lobbying the issue.

Feel free to contact me,

Anthony Schmidt

Let me say that I am a rather average college student in the middle of the bible belt, the most conservative section of the USA. I attend media class after media class every day, and spend my time writing papers about such subjects.

Let me also say that I am also an artist, filmmaker, writer, and reviewer. I deal constantly with the purported 'cleansing of materials for public consumption to prevent harm to the general populace'... in other words, censorship.

I fail to understand why of all first World nations we in the USA are the most backward progressing nation in the area of personal moral perception. The basic idea being that what one person and or group perceives as god and or bad morally, is not what another group and or person perceives as moral. It is a basic idea of personal liberties, to decide without a dictatorial commission what an individual considers to be moral.

Progressing to the crux of the matter, under what purported moral dictum does the Commission see it necessary to imprison owners of Internet Smut sites? Or for that matter to censure a closure of site? Is it a fun game to ruin peoples business? Yes, to select groups their sites are offensive and immoral, but like all those sites say, "Do not proceed."

There are cases where people would find a commission that decides to dictate morals to others to be in and of itself criminal, and repugnant to society. As the great man Jean-Jacques Rousseau once said, "Censorship may be useful for preservation of morality, but can never be so for its restoration." Watch upon who's toes you tread for a step too far has irreversible and often undesired repercussions.

Censor, I mean, Protect the populace with ignorance, all you will... I know my words fall upon deaf ears. I've written organizations before and found that they live in tiny closed off little worlds that cannot, nay will not, admit new thought provoking ideas in.

Signed
Grey Jedi

In addition, software blocking of internet sites is unnecessary, any computer savvy parent should already know how to access the appropriate files to discover where their child has gone. That and many parents falsify accounts for their children now because of the annoying privacy invading methods used to block 'questionable sites.

To The Commissioners:

I would like to express my concern regarding the Children's Online Protection Act. The bill does not identify or define what an "adult identification number" is, nor does it identify by what authority these adult identification numbers will be assigned. The bill's use of the Miller 3-prong test to determine what material is "harmful to minors," is not applicable to the Internet as a broadcast medium. The "contemporary community standards" of what is acceptable and what is not are not applicable to a medium that is broadcast world-wide. The use of the term "average person" is not useful when applying it to judgements that are inherently personal and not in any way objective.

The bill leads me to believe that its enforcement will lead to an erosion of adult privacy by making it possible to track adults who are accessing information that is "unacceptable." While I am sure the government has not intention of tracking people who engage in such behavior, this legislation's use of "any adult identification number" suggests that this sort of surveillance will be done later, as do the other two means of ensuring that adults only are accessing the information via the Internet.

I understand the Government's conviction that there is information that is inappropriate for children that is made accessible to them via the Internet, however it is not in the Government's best interests to attempt to subvert parental authority by removing a child's access to this information through legislation.

Signed,

Christie Robbins

To whom it may concern,

It is my understanding your commission is currently meeting to discuss ways to prevent children from accessing web sites with inappropriate material. One possibility you're currently exploring is new domain names for adult material. While this might have some minor positive effect, I feel this is the wrong approach. First of all, pornography is like any other business and will decline to disassociate itself from other .com businesses. Secondly, there will always be those sites that will try to gain the underage audience back by associating with the .com domain name. And as the Internet has repeatedly shown there are just too many to keep track of and enforce legalities upon.

In this light, allow me to propose a suggestion. The <HTML> standard is still young enough to install a new <tag> within the a document code, this tag could be used as a site rating. The web designer could then assign the site a material rating that reflects its content. This would be similar to a movie rating, an example entry could be <rating>G</rating> or more importantly <rating>MA</rating>.

Allow me to explain what I feel are the benefits of this method. Firstly, this offers the potential for total child access prevention, for web-browsers need merely to offer parental passwords that toggle the browser's own access to adult content sites. If the browser lock is on, the browser simply refuses to access a site whose HTML document includes a bad rating. You're probably thinking of the situation were sites purposely give their content low ratings so that all might access, or even no rating at all? As far as a low rating for adult content, that is something that could be informed by law, if sites are to use the rating system, obviously some legalities must be imposed to prevent the systems abuse. As for no rating, freedom of speech demands this be acceptable and I too believe it should be, but again browsers could EASILY be established that simply do not access sites without a rating, leaving it in the parents control to acquire these browsers.

That is my suggestion, I feel it is one of the only true alternatives without compromising our rights to freedom of speech. If the commission could swiftly consider this option, the rating tag could be soon on its way to standardization. Thank you for your time and consideration, I look forward to the day our children may browse the web safely without compromising their liberties.

Sincerely,
James Gilbert

Dear Members & Staff:

Let me first take this opportunity to congratulate you on the success of your hearings June 8 on protecting children in the online environment. The wide scope of subject matter and opinions expressed will help frame the policy discussions that we hope will bring about a more safe and enriching online experience for young people in a wired world.

My concern is child pornography being traded one the internet. In the chat rooms of MSN.COM there are chat rooms dedicated to the trading of child pornography. These chat rooms can be found grouped with the chat rooms for teens.

The online chat rooms at MSN.com are infested with pedophiles. There are no sysops to supervise young people as there are at AOL. I visited the "1_preteen_pics_trader 1" chat room where I observed commercial web site operators enter and solicit what was purported to be child pornography. Rape photos of girls under 12 were in particularly high demand. This goes on as a commercial enterprise daily. As there is inadequate supervision minors are also in these chat rooms, sometimes offering "self pics" of themselves.

These matters have been reported to MSN, which took 28 days to respond, as well as to media outlets. I have left a message at Cyberangles as well, but to date, this activity continues unabated. The material being openly traded is of the most graphic sort with minors.

I oppose censorship but children must be protected. Microsoft has done nothing to prevent this activity.

James E. Morrow

To whom it may concern;
As a uncle of three,and computer operator,which my software is Microsoft Windows'98 second edition I'd like to suggest the followin ways to prehibit non viewing of non-juvenile oriented websites.

1.If the adult never visits the websites,nor bookmarks them by control"D" the website addresses are not as obvious to the kids.

2. I also have all Microsoft security updates within my computer,including that of June 02,2000,You can download these by left clicking on "tools" in your internet browser,go down to windows updates right click that,then view,check,and download.you can check your security @www.grc.com

3.NetNanny from cnetdownloads.com click on browser software,find netnanny,and download.

However this will not stop these cites from sending e-mail if before installation of above the operator has already visited these non-juvenile oriented sites,example Gaytradition.com,and others.I also have a firewall from mcafee.com,and if I even think that one of thes websites have been visited I check my computer browser favories,if found delete them,and go to mcafee.com cleaning them off the harddrive.Lastly,If I get an invitation email I click on reply in my email browser telling them I'm Not interest and direct them to block it in the future.
Per your Times-News story this Monday,June 12,2000.
Willie Ray Bowen

I have long stated that we need the designation:

.prn

for porn sites. There is no need for mistakes when searching/surfing/browsing the web. Since everyone has the RIGHT to do as they wish, then let there be a category for those who choose "adult" information.

Linda Phifer,

The following was sent to Senator McCain germane to his attempt to require libraries to install filtering software in order to continue receiving federal funds. Most of my comments to this commission are covered in the e-mail to Senator McCain:

[Senator McCain] I'm writing to encourage you to rescind your amendment to H.R. 4577 (No.
3610). I have sent my two senators a request to vote against your amendment. Although I believe your intentions are in the right place, that you really want to protect children, this amendment is not the correct approach and, possibly, even counter productive:

1. It's unnecessary in most instances [to require filtering software], for example here in Allegan.
Consequently it is an unnecessary intrusion by federal government into what should be a local decision. Contrary to popular perception perpetrated by the media, many libraries do not have a problem with internet usage.

2. As recently demonstrated, many filtering companies filter out or are capable of filtering out business competition, political beliefs that go against corportate policy, medical information, or social beliefs in addition to pornography. With the rate of change on the internet, how do we expect libraries, especially small poor libraries, to keep up with this filtering requirement? This amendment will force these same poor libraries to forever allocate funds to keep up with these changes. Will Congress provide the financial support? Is Congress willing to provide the funds to ongoing monitoring of the filter companies? Quis custodiet ipsos custodios?

3. There are better methods for dealing with inappropriate use than mandatory filtering which, in reality, only provides the illusion of protection. It is my guess that the business people involved in pornography could care less whether libraries filter or not and, perhaps, may do better if filtering legislation passes because circumventing the **protection** provided by filtering is no big deal. Whereas the honest local citizen may never know what additional information was withheld by the filtering company that, perhaps on a whim, decides to block all Michigan information for a day (example exaggerated to make a point).

Please do what is right and withdraw this amendment which will hurt most those libraries most in need of E-rate discounts. This intrusion by the federal government is not necessary nor appropriate. Ironically, a vote for this amendment will do nothing to protect children and will only provide an illusion of protection. Trust local communities to take the action required for their specific needs. One size does not fit all. I hope that you also reconsider the Children's Internet Protection Act; I suggest that this issue is best left to local communities, many of which have dealt with eliminating internet pornography use in intelligent, thoughtful, and effective ways that really do help and protect children.

Ed Spicer

I am an Adult Librarian in a public library in the Richmond, VA area. I am continually concerned about unsupervised minor children using our Internet machines. The Internet in our Children's section is filtered. However, few self-respecting children over the age of 10 or 11 want to go to the Children's Room . It is for babies. Children come after school, completely unsupervised, and spend hours on the Internet in the Adult Room. We have no time limits or sign-ins. Other than simply asking the child how old he or she is, we have no way to determine how old they are. We try to send younger ones to the Children's Room. They don't want to go. I think parents erroneously assume that their children are safe in a public library. Parents have no idea what their children are viewing on these Internet workstations. The names the kids use in chat rooms are frightening. Thirteen and fourteen year old children are calling themselves "Hotstuff," "Sweet Lips," "DeadSexy" ad nauseum. Many nights all 17 Internet workstations are being used exclusively by adolescents. With one person staffing a large room with 3 telephone lines, there is no way we can adequately supervise what these kids are doing. They are definitely not using the public library for its intended purpose.

While it is good to see your commission studying this difficult and important question, it is an unpleasant surprise that public and school librarians are not included to and significant degree in the commission or in the list of witnesses. Librarians have more experience working with children, the Internet, and filtering issues than anyone. In Virginia in particular public libraries have managed to provide children access to the Internet in the manner dictated by their communities. The Loudoun County case drew national attention, but numerous other library systems have chosen to filter or not to filter and lived with those decisions. I hope you will consider consulting some of us who work on the front lines of this social battle.

Cy Dillon

Dear Commisioners,

I am one of many youth who have un-knowingly accessed as site with pornographic material. As a victim of deception, i clicked on a link.
If i were to start a petition against this, you would find that millions of under age teenagers have stumbled upon sites with pornographic material.

Many times youth go out looking for it. This is something that comes with harmones and maturity level. This is something that young children could easily acess just by mistake. I hope you to take this into consideration.

If willing, i would ask that you let me start a petition going against this, just for teenagers and children under the age of 18 that have stumbled on or found web sites with pornographic material. Thank you and God bless,

Justin Johnston

My company, InForAll, Inc. has taken the technology you are discussing to the next level. We recently introduce a product called iForAll that uses peer to peer technology. This technology allows apparent to view exactly what the child sees on the child's computer. Yes, we incorporate RASi, provide blocking and key word filtering, but the advantage of iForAll is its real-time remote monitoring capability. A parent can be anywhere and be connected with their child. IForAll can see all Internet activities (web, chat, email and ftp). This is only part of the program. iForAll also allows the parent to have either a one-way or two-way conversation with the child. The parent can even disable the child's computer. As a final family feature, iForAll also includes a family communication center that includes a family calendar, address book and a personal information page.

We feel this technology is the future of child Internet management software. Passive program do not work because they need to keep updating themselves. These updates are never 100%. Passive software solutions also allow parents to abdicate their responsibility of being the protector of their children and moral lighthouse for their children. iForAll keeps parents involved. Passive software and government regulation does just the opposite.

As you can see by our address we are located in the DC suburbs. If you would like a demonstration of iForAll or if you would like a copy delivered to your office, just call.

Safe Surfing!

Tom O'Connor
InForAll, Inc.
Silver Spring, MD 20904

Hello, I was wondering: How can one group of people decide what is "inappropriate" for another group? It's obviously wrong to judge someone by their age let alone treat them like others in their age group.

I admit it, I "consume material" that most everyone at the COPA deems "inappropriate", but I also "consume" other material most would find intelligent and moral like Oprah. In my view, from a 15-year old whom you are trying oh so hard to "protect", it would become much more benificial recommending minors to use their heads, rather than preventing them from not using their heads.

Now it comes down to this:

I'm not a porn addict,
I'm not a child offender,
I'm not a "pervert",

Are you going to tell me that I'm wrong, only because I'm 15? That would be really prejudice and insulting if you were to do so. Thank You.

As a computer store owner and computer hobbyist, software filtering is not as preferential as ISP filtering due to the ease with which it can be circumvented, the incompatibilites with other software, and that its not updated easily. If all ISP's offered filtering that would be immensly helpful but larger providers like @home cable services don't, and, the software filtering they offer doesn't work very well.

I really like the idea of designating a series of IP addresses to the porn industry, though not sure how practical it would be to implement. Not sure if implementing the idea would be easy as ISP's have an IP address associated to them and the x-rated sites they host would be associated to their IP address along with all the non-sex related sites they host.

So, due to its ease of implementation, the .xxx or .sex extension is preferable in that its implementation is easiest to do. Internic should be persuaded to implement this extension for each country to determine if they want to use it. Sure some countries may not, but its a step in the right direction toward simplier means of filtering porn by password protecting access via the browser.

Another reason to go with a red-light alternative to a green light is that most adults do not frequent x-rated sights, and, more importantly some do because of its easy access but would not if the temptation wasn't so available - like myself!

There are now reports about growing sexual addiction based around net-porn that could be curtailed by some simple changes. The internet with broadband cable is easier to use than going to your public library. However, imagine the outrage if the library provided porn and it was mixed in all catagories from fantasy to fiction to children's books where children could very easily check out the books.
Or imagine T.V. with smut intermixed on various channels at all hours every day where all you had to do is to on the t.v., flip through some channels and your kids can easily watch porn. The internet is almost that easy and porn movie clips are available free to watch now on the net.

If some regulatory agency can keep porn from public airways, why can't the same be true for the internet. I pray that an easy-to-use realistic approach becomes available shortly!

Patrick Ewing

To whom it may concern (Child Online Protection Act Commission):

I have recently read, with interest, the proposals for Internet Protocol address-based content delegation discussed on the August 4 commission hearings. I wish to raise some serious concerns about these proposals, which I think are technically misguided and very probably infeasible.

It is unfortunate that there do not appear to be many (if any?) people associated with the commission who have direct experience with the technical management of large Internet or IP-based networks.

While the recent proposal to allocate a "small portion" of IP address space for specifically content-based "child protection" schemes - whether by allocating certain addresses specifically to X-rated sites, by allocating certain addresses specifically to "kid safe" sites, or by doing both - may sound appealing simple, it would likely prove disastrously difficult to implement.

The Internet has long been suffering from an ever-increasing Complexity f routing tables - the critical "maps" which specify how to get from point A to point B, given that those points are known only via their Internet addresses. Because of the complex and cooperative way in which these routing tables are calculated on a minute-to-minute bases, the present need to redistribute or "carve up" some very large blocks of addresses which were originally intended to be contiguous, and the need for each provider to filter invalid route announcements, there are already real problems in reaching certain addresses by way of certain Internet providers. (I am drastically oversimplifying here, as should be bvious.)

At any rate, the Internet Protocol addressing scheme was designed on the assumption that blocks of addresses would be roughly correlated with geographical location, and be specifically and closely correlated with network connectivity. A current biggest problem is generally assuring the reachability of small blocks of IP addresses, especially those which have been suballocated from large original blocks of addresses. (For technical reference, I am referring to the ongoing subdivision of unused "Class A" address space.) Any group of less than 256 contiguous addresses (a "Class C" in old terminology) from any source is nearly guaranteed to be unreachable from other Internet sites; in some cases, blocks of less than *4000* contiguous addresses (a "/20" in current terminology) may not be reached from all providers if they were subdivided from a former Class A block.

Do you begin to see the problem in adapting your IP-address based proposal to the Internet and web?

First of all, it would have to pass the approval of the various international boards which administer the allocation of IP address space,
which currently work on largely technical grounds and have mostly avoided
political involvement.

Second, if implemented, it would require some party to take over management of some IP address space - a highly technical process - and dole it out to applicants while satisfying itself of both their technical
competence to manage the space, and their intent to comply with the content guidelines.

It would also probably require individual IP address assignment to each
individual web site, which is against current policy for IP address management in the Americas. (In the future, it is expected that most web sites will not even *have* a unique IP address but may exist as what is called a "hostname-based virtual web server".)

Moreover, due to the shortage of current IP address space (which will not be alleviated any time soon) it would not be feasible to give any applicant much more than they actually needed or proposed to use in the near-term. You can see that this conflicts very badly with the need mentioned above to allocate space to Internet providers or sites in a minimum of 256 address "quanta" as listed above.

Finally, given all the issues in management of route maps that I have alluded to above: the end result of this proposal, if it were implemented, might very well have the effect of guaranteeing that most of
the sites which wished to be identified as "kid-friendly" or "kid-safe" end up "dropping off the Internet" and becoming inaccessible to *anyone* due to the difficulty of getting routes to them accepted, once these addresses are subdivided into tiny blocks scattered around the whole Internet.

In short, I think this proposal would be disastrous for purely technical reasons, however well-intentioned, and whether or not it is legally
viable. I strongly urge you to reconsider.

Should you wish to consult technical experts, I suggest you consult some authorities on current Internet Protocol routing policies and Internet Protocol address allocation. One such group you may wish to contact is the North American Registry for Internet Numbers (ARIN). See <http://www.arin.net/> or contact hostmaster@arin.net for more information on finding an appropriate contact person for further technical discussions.

Yours sincerely,
Clifton Royston

Commissioners,

Perhaps it would be better to let the problem of control of children's access to the web be solved by the private sector. Given the demand for this control, as evidenced by the existence of your commission, it shouldn't be long before kid-safe ISP services are offered. Connection to uncensored ISPs can be controlled in the home by simply not saving the password to the uncensored ISP in the browser or connect software. Kid-safe ISPs can offer browsing of approved web sites by selected keywords or hypertext, as AOL does, and not allow general access by URL. They may even be able to charge a premium for this service.

Chat rooms are another issue, but perhaps a kid-safe ISP could charge customers to have people monitor chat rooms under its control, thus providing some protection and making some money in the process.

I think government intervention in the Internet domain should be *very* carefully considered, and should be a last resort. Perhaps one way government could be helpful is to certify an ISP as meeting "kid-safe" requirements. The development of these requirements and the certification of ISPs would be a great service to the Internet Community.

Yours truly,
Robin Uyeshiro

Hello,
I am an adult webmistress. I have been following the COPA in the news and I have not seen this particular problem addressed by COPA or anyone else for that matter: newsgroups. Anyone possessing MSIE or Netscape and a dialup connection can have access to thousands of hardcore porn and bestiality photos delivered right to their PC every day-free. No credit cards needed. There's no age check/verifier or password protection involved. And the same can be said for egroups.com . Underage individuals can access all this material, and the proposed 'red light district' for porn sites would do nothing to stop the underaged from access all this material free from news servers or egroups. Personally, I believe all newsgroups should be prohibited from posting binaries. But it may not be feasible. It is one solution anyhow.

Thank you.

Sincerely,
Webmaster

Article in regards to:
(ZDNET)
A government office on sexy sites?
A federal panel examines how to protect youngsters from online pornography.
Is a government rating office the answer?
By Ben Charny, ZDNet News
August 3, 2000 3:34 PM PT
http://www.zdnet.com/zdnn/stories/news/0,4586,2611649,00.html
SAN JOSE, Calif. -- Librarian Jean Armour Polly was able to find what she wanted when searching for filtering software to put on her school's computers. But she never found what she really needed.

___What the gov't SHOULD have done in the first place. was say that Porn webmasters/sites had to put; perhaps a certain snippet of [HTML] code in the header of the HTML document so that filtering software could block that out from youngsters... Webmaster's that didn't include that code could have been liable for showing porn to minors. If, and when that happened. But since the filter would only block minors. It would

1) Protect minors and;
2) Protect webmasters from liability without having to go through the hassle of dealing with AVS's (Age Verification Systems... Which do the credit card checks...)

This thing I talk about, would be simply how the rating system is on TV.. When the New TV's come out with the V-chip... I think you can block all the TV shows that are above a certain rating.. Well this STANDARD would work the same way... All sites would put this coding, so filters can pick up on it... And this would ***ONLY*** block sites kids which have no business at the site... But this code wouldn't infringe on the web site's paying customers...
--

And it wont cost webmaster ~$70 for having to switch from a perfectly fine [Dot]Com to a [Dot] XXX or whatever the new domains are.

If you try to force webmasters to move they will kick their heels in the sand and say that it's censorship for making them buy new domains. Last time I checked also ICANN or Register.com and the like would NOT give away the .XXX domain names either because porn site's aren't non-profit they are businesses... Thus will be charged accordingly...

2nd post:
Does the Net need a 'red-light district'?

A red zone for porn and a green one for kids were among the ideas tossed about at a Child Online Protection Act hearing.
By Ben Charny, ZDNet News
August 4, 2000 2:39 PM PT
http://www.zdnet.com/zdnn/stories/news/0,4586,2612074,00.html

SAN JOSE, Calif. -- Zoning rules and regulations like the ones used to carve up cities could soon be making their way onto the Internet.
--
__ People in here have used newsgroups right? Have you seen something like this?

"x-no-archive: yes" In the first few lines of a post? Which is supposedly to have your post not "cached" on sites like Deja.com etc... Well use a variant of that.. That Filters and browsers can be trained to see something like "x-check-adultsite: yes" or something like that.... No need to infringe on someone's freedom of speech making them have to **buy** a new domain name because you don't want to see their content. Thus you move them to the far reaches of the Internet (Censorship)

With this simple HTML tag fix, webmasters can stay right where they are, and will require minimum effort to change from non-compliant against minors... To against minors, and compliant... Filtering companies can stop trying to keep databases of sites, to stay away from... etc. There's no need for that and that would be a never ending task.

[Dot]Kids I don't think will be a good idea. That just gives Stalkers/Pedaphiles someplace to hunt down.

The Internet is not a playground... Just like you can't censor what's outside your door what makes the government think they can censor the Internet to infringe on someone because of disaprovment with their content. If government doesn't cost webmasters a lot of money and heartache like the .xxx extenstion then they may help instead of rally against everyone. Example: You take the thousands of adult side domain names and channel them in .xxx or .adt And I bet After sex.xxx or sex.adt or the other 'common names are taken' you WILL hear someone saying they don't have any good pickings thus want this law overturned... The gov't needs to stop making laws that are made to be overturned because sooner or later when they *do* want to make *MEANINGFUL* legislation to "protect" minors. It would have been already ruled out from a prior case. Make laws as simple as possible don't complicate things... Just like the US got the cybersquating law upheld in more international places they could get something like the proposal I outlined supported... As far as I know a few of the Asian countries want to/have put in their own legislation... This proposal could help them too...

I must admit... This idea for the "x-check-adultsite: yes" isn't completely mine... I thought it through mostly based on the FCC's proposed V-chip which will block programming over a certain level should parents use the chip...

It has been stated repeatedly by the government that, they want little involvement with regulating the Internet. While attempting to not interfere in the everyday operations, we find a commendable effort, it is near impossible to not take some sort of role. If individuals and companies (In this case webmasters and surfers) where able to deal with those that "cross lines" or break laws, then we wouldn't need police. Just not going to happen, there will always be those who do a poor attempt of thinking they are beyond whatever rules that are in place. No matter how hard many of us try, we do not have the power or authority to prevent it.

The only downside to Government interaction is many times, they are not fully aware of what they are regulating. The COPA law has many positive attributes but several negative ones as well. There needs to be almost a sub-government working on the Internet as a team to ensure things work smoothly together. In the paragraphs that follow, I will explain who I am followed by what is both strong and week about the current laws. I hope the information will be able to help you with your final report in the later half of October. I apologize for not providing this information sooner, but as you know it takes time to gather information and layout a resolution. If anything needs clarified or re-stated, I will be more then happy to respond and assist any way needed.

My actual name is Steve Dickson, I reside in Indiana and a father of four girls between 5-11 years of age. While working on-line over eight hours a day, I have seen pretty much every aspect of the internet. Everything from <http://www.yahooligans.com/>http://www.yahooligans.com/ which is a great children's search engine, to a site I just reported for child porn. I "talk" to people on the ICQ chat program all the time and have no problem asking them for their impute on any given topic. All this combined has led me to the information to follow

It's been proven time and time again that Child Protection programs (CyberPatrol, NetNanny) are not as effective as the should be. Letting parents depend on these programs alone in negligent. For example, all my children have been on computers for years, my youngest (Age 5) is on our other machine as I type this and has computer lab in school every week. Many parents just don't have the knowledge our children do. I was self taught just like millions of others, I managed to get into computers in the very early 90's so have had a long time to study. Over the years now I have heard things as simple as "How do I find ____ on the internet". I look at the message dumbfounded for a moment then reply "Have you tried a search engine?". Most times they haven't. Now add that to the concerned parent "Protecting their children".

While the government is going to have to make things over complicated so that there are loop-holes (Such as posting nude pictures of children for adults to spend money to

see isn't illegal. As long as it isn't hard-core! That's truly repulsive, but it's "The law") The answers are all very simple.
1. AVS (Adult Verification Systems) Some of these need regulated do to, it can be easy to acquire a password for them. This does tend to be the most viable solution. No content over PG13 without it. Doing so would constitute the violation. This would drastically reduce children's exposure, while focusing on how exactly to help cut down on things like false meta tags (Used in web pages to help search engines index a site) Example: I did a search for Comicbooks. the third link was nude pictures of Pamela Anderson.

2. It was recently stated in a news article that "It doesn't take a rocket scientist to make current laws work on the internet". 100% correct! Adult Magazines arrive in a black bag or is behind a counter. Adult videos have signs have "Must be 18/21 to enter", this is done on adult web sites, the problem is who is at the counter making sure they at least look old enough?
Think about it for a moment, the site above not only broke the law by exposing the site to children, he used false advertising to do it.
3. It can't be just that simple, it will prove an ineffective as everything else done to date. Major crackdowns have to be made over the entire internet and the best place to start is by working with willing Adult Webmasters and cracking down fast and hard on illegal sites.
Defined: I have a database of over 1100 webmasters, all of which can have an AVS system in place on their sites in less then a week. Many "Mega pay sites" have edited tours and openly promote various AVS services to the webmasters who promote them. I have studied "Partnership programs" from many industries on the internet, the "Adult" programs beat anything else hands down. Better user access, for more detailed and extremely easy to use. While the government allows people to post nude children on the internet, Adult programs are repulsed by it. Free ISP's, affiliate programs and even TGP's (Thumbnail Gallery Posts. 1,000's of hard-core pics for anyone to see updated everyday). Many won't allow over use of the name Lolita, which is the name of a book about a man who "Fell in love" with a 12 year old little girl named Lolita.

It's all really simple to compile together, while complex to maintain to an efficient level.
I. All sites with Content deemed over PG13 must be AVS protected.
a. This includes "Free servers" who have the banner position at the top and bottom of pages.
1. Free servers must provide a "Secured" folder for webmasters to place their protected content. This is very simple process to do, so no one can complain about "resources and time". That's just smoke and mirrors.
2. All webmasters will be able to be properly identified with ease due to they have to give their personal information to the AVS system in order to be paid
II. Currently non-compliant sites would be fined up to $50,000 per day and up to six months in jail. That's not overly viable "As is"
a. Not all webmasters are on-line everyday; thus, may not get their e-mail everyday. They should receive the first fine just because the did break the law, but should have a "Grace period" before it constitutes a repeat offense.

b. Many webmasters on free servers will never be able to come up with the first $50,000 so forget about any additional.

1. As stated above, the adult industry has the best cgi-scripts for tracking and reporting then any where else on the internet. With this in mind, all should be held accountable. With several programs I have studied, it is VERY possible to track exactly where hits came from for affiliate programs and web servers have total access to things on their servers.

c. The webmaster is the single largest entity responsible for the content they post and where. They should receive the full amount of any jail time issued. In addition, there will be records of how much they have earned and that will estimate how much of the fines they should pay.

1. The servers be it a free or paid hosting is aware of how many hits a site gets and to what pages, they have the ability to terminate any account with ease. I see no reason why they can't police sites for wrongful activities.

2. Affiliate programs also have full access to where hits come from. It is far more difficult for them to regulate due to webmasters are on many different servers. Most of those servers are not regulated by them and they would have to contact both the offending webmasters and the server they are hosted on.

3. Many webmasters will quickly become compliant upon receiving the knowledge that they can and will be charged. The servers should be the primary target for cash fines, and affiliate programs to a lesser degree. None can complain about "Additional costs" of operating. Most brick and motor stores have loss prevention, expensive surveillance equipment and other things to do similar jobs. While it will be more costly for affiliates to regulate that many webmasters, they almost all have the same clause. Violate the terms of service and the account is canceled without payment. That
could be nothing or in some cases $1000.00's.

d. There are a good number of webmasters who would like to be more compliant, but thanks to no law enforcement of any kind, it is difficult for them to do so and still "compete" It's easy to just blame one sector of a problem, but that is both unfair and not effective.

1. The Adult industry as a whole can be compliant and strive to obey the laws and it will do a lot of good. They can't do it alone. What is needed is a central location for the adult industry to help each other. This happens all the time, I can provide countless links to web sites ran by multiple sites for a common reason. If sites, surfers, webmasters and such could log in and provide violators web address then, many sites could ease the strain of finding them all.

2. There are plenty of "outside" factors that will effect the efficiency of any law. The current joke with Napster is a prime example. Many servers won't allow "Complete" MP3 files. Affiliate programs like Amazon.com will cancel an account if they discover a site makes complete songs available. ITS THEFT. There is the argument that people have been sharing files with friends for years. Very true! None of us have ever shared them with 30 million of our "Closest friends". If Napster isn't shut down, then why not make Warez legal? If you can steal music, steal programs. That leaves the door open for password trader sites, which is stealing services and directly allows children to get passwords to porn sites.

3. Mistakes happen, with any medium, so should not be treated in an over zealous

fashion. A blind link. tricks a person from leaving where they are in order to go to a site they had little or no interest in. Upon reading documentation on false advertising, you will see this fills many of the "requirements".
<http://www.lawnotes.com/false_advertising.htm>http://www.lawnotes.com/false_advertising.htm
4. Hacking a computer requires entering a home or business threw the phone lines and proceeding to read or destroy private property.
<http://www4.law.cornell.edu/uscode/18/1030.html>http://www4.law.cornell.edu/uscode/18/1030.html
5. The Internet is like no other technology in the history of mankind. The United States Government should be in charge of all laws governing the Internet in the United States. Allowing individual states to regulate them selves while have the sovereignty of the union is a great factor in what has propelled our country to where it is today.
There are federal laws that supersede the individual states and this should be true in dealing with the internet. More work, complicated laws and other things can be avoided if there is only one version of a law. Gambling, Adult content, taxes or anything else. Example: Texas banned Ford from selling used cars on-line to consumers. The car want to retailers in the area and all inspections and taxes had to be paid. I would be upset if the congress from Indiana pulled such a stunt.
6. The standing law in regards to "Adult content" while using children needs revised.
<http://www4.law.cornell.edu/uscode/18/2256.html>http://www4.law.cornell.edu/uscode/18/2256.html Just paying by credit card to see nude children, "Hardcore" or not, should send up red flags.
7. Credit Card companies are multi-billion dollor ego maniacs. Their sole concern is making money, with little to no regard for their clients. They impose stiff fines for excessive charge backs. The leading industry for this is Adult Websites because a portion of consumers find it easy to do. IBill and others have software installed to detect card numbers that make a habit of charging back and refuse to except them with their clients. Credit Card Companies should be forced to use similar software, fine the companies that are at fault, but repeated service thiefs shouldn't be allowed to "refund" every other day. There is a lot less profit not fining innosent companies so to date have no interest in being honest about it.

Without all of the above working together any individual law will be substantially less effective then it could be. There are of course much more in-depth factors, but they are impossible to portray is a single e-mail. As stated in the opening lines of this message, Myself and many others are more than willing to contribute in anyway we can. We do not represent any one company or industry, so can remain neutral, while wanting to protect children and the rights of legal adults. A great deal of us understand the workings of the internet, but more importantly can provide the perspective of what "Actually" goes on around the internet.

Sincerely,
Steven G. Dickson
(219) 389-9805

Dear sir of madam,

Thank goodness for your committee. I support restrictions on children's access to porn on the Internet.

I have a method that will help reduce access by minors to material that is harmful to minors on the Internet. Maybe we should make computers cost more than $200. I can't think of any kid that has $200 for a computer so this would keep most of the kids off the net.

Or the children could impldment "parent" version 1.0. This is a program that is rarely used these days and once activated would rid children from viewing material that is harmful to minors on the Internet. It appears that most the "parent" programs are still in beta and require millions of plug-ins to keep children from viewing material that is harmful to minors on the Internet. It seems easier to fix the ONE "parent" program than it is to fix the MILLIONS of plug-ins to rid children from viewing material that is harmful to minors on the Internet.

I was just reading a news report about more police on the web has any thought been given to retired P.O. I am a retired New York City Police Office that has time to spend on the web you could make these retired officer marshal and you could have a lot of *experience to help in this fight*
it just a idea but with some merit I think
Craig V Hewitt prophecy@ispchannel.com

In the report, the commission cautioned that governments need to "pay competitive salaries and benefits" to retain Web-savvy cops in an era where technical skills command high dollars.

Since it sounds like high paid web savvy cops are wanted, why not hire a minimum number of cops to serf the net for child porno and let them check up on sites which are turned in by ordinary web serfers who are paid rewards when a conviction occurs. This seems to me to be a more cost effective way to spend money for salaries.

Thank you,
Gerald Erikson
sgminer@gci.net

As I'm sure you've heard in testimony, biometrics, will be the future of online authentication.
I own a company called Age Protector who has two partners that will allow us to age authenticate on the Internet using a biometric voice sample and Driver License records. This web-based service will allow adult oriented sites to keep minors off, very simply, and across all platforms.

I'd very much like to talk to someone at COPA about this service. The vendor downloads were specifically about filtering, ISP's and Labeling technologys and don't really apply to this service.

The voice service is up and running and the commerce beta test is going on as we speak.

Who would be a good contact to follow with or submit a vendor proposal?

thanks

The solution is so easy it is a wonder that it has been overlooked:

Move all the pornography to a new domain called .porn

Credit card the access for age verification and that's the end of it.

Hi,
I have a terrible problem that I don't know how to handle. Please help me! My son, who is a minor, keeps getting porn e-mail, of course they say he can't get into the "hardcore" stuff without a credit card. (If what they show isn't hardcore, I'd hate to see the hardcore stuff!). His e-mail is through hotmail and they have a feature that you can "block the sender". Unfortunately, tho, it is a different sender each time, but everytime it is from an earthlink address. Here are examples:
from e-mail - twinkieman@uit.no
web site -
ction=http%3a%2f%2fhome%2eearthlink%2enet%2f%7ejmcquire627%2fsexy%2ehtm
web site - http://home.earthlink.net/~jmcquire627/relo/sexy.htm
from e-mail - nsuthe@weintl.com
_action=http%3a%2f%2fhome%2eearthlink%2enet%2f%7ettucker60%2fsixy%2ehtm
There are several more, but I e-mailed them to report@internet-police.co.uk and them blocked them and threw them away/deleted them. But the internet police never let me know that they are doing anything about it and my son is still getting them.
And did you notice that all the addresses have "earthlink" in there somewhere. That should tell us something, hey?
And I noticed that all the addresses I have to copy down by hand and then come to either you or the internet police and copy it by hand into the e-mail I send you because it doesn't forward on it's own. That tells me they are ashamed of their actions.
O.K. , well... enough said. Please get back with me and tell me what to do.
Thanks
Rachel

I've read the COPA law in full detail and have reached the same conclusion as the one I had before I had read it. It's too broad. I am 15 years old and I'm outraged by the fact that an online community I used to visit has been completely changed around to some pathetic excuse of a website because of the COPA law. The community was simply an area for children of all ages to submit drawings and comics to the website... the website reviewed all of the comics they received to make sure they weren't offensive or harmful in any way... and they also had a message board, where children could interact with eachother and post comments on their comics. This board was also monitored, and not once in my 7 years at the community have I seen ONE harmful post. Now, because of some law that's supposed to keep me from viewing porno sites has kept me from viewing a CHILDRENS ART FORUM. I'm not even sure if it's necassary, but I've known the people who run this community not to be threatened with 6 months in jail and/or 50,000 dollars for every day they don't comply with a law that wasn't even made for them. Because of COPA, before you send a comic, you must get your parent to e-mail them with permission. Afterwards, they review the comic and put it up without your "screen name" (an AOL thing, like a nick name that you go under. Example; my real name most definately isn't "Metemphere")... why would I want to put up a drawing, if I'm not going to be acknowledged for the work I've done? Also, the message boards were changed... now, when we post a message, they review the post before we post it (which means the 100s of posts that go in don't actually get seen until 3 days later, which is highly neanderthal). Also, when they do review it and post it, OUR SCREEN NAMES AREN'T BY THE TOPIC. This means it's an anonymous message board! Once again, I ask you... why would I post a message when I won't even be recognized for it? Thanks for bringing interaction to a new level. The nonexistant one.

Metemphere
"Sooner or later, your legs get weak; you'll hit the ground...
Save it for later, don't run away and let me down..." - Harvey Danger

The COPA Commission is doing a fine job but is too lenient using the same weak laws that are allowing strip club billboards on our highways and roadways with no resource to filter or block them out. These billboards glorifying the sex trade industry are deliberately aimed to have young boys grow up thinking of girls as sex objects, and to coerce young girls toward perverted behavior The sex trade industry is not stupid; they know exactly what they are doing and are succeeding with their goals to be in control. They frustrate and eliminate parental supervision by forcing children to read age inappropriate material. Please don't let that happen on the internet. This is not a time to be introducing more lenient laws with a business marketing sex to minors.
Most Sincerely, Lynn Sweet

There is only one answer to the question 'How to keep children safe from sex sites on the Internet.
Make it the responsibility of the origination and not the reception to limit pornography to adults.
How to do this. ADULT CHECKS and confirmation BY POST of someone wanting to join such
a site. NO titbits for children to look at.

Without any requirement of age (except my own guarantee that I was of age!) I was able to see and read examples of ROLE PLAY RAPE, ROLE PLAY ABDUCTION, BONDAGE, with uncontrolled links to MOCK EXECUTION and SODOMY. (The site was http:\\www.abduction.com\redsrealm\ - but there are plenty more). The URL says it all doesn't it?

What about protection programs like NetNanny - in computer matters children are mostly more educated than their parents and the computer is often assigned to the child's bedroom - formatting and re-installation of OS - by-passes ALL safety protacols!

No one wants their children to see PORNOGRAPHY so lets not be cowards lets have the guts to do something NOW!

John Spooner UK

Hello,

If in any way possible, I'd like Commissioner Donna Rice Hughes to read my opinion on the matter debated by the COPA Commission at http://www.copacommission.org/

I don't have any link to porn websites in any way whatsoever -- I want to make that point very clear. It appears a lot is being done to sue porn sites using children as models and I believe those site operators need to be caught and dealt with on a very severe basis. As for the "adult models" porn sites, it seems all models are very much willing to pose. Such a point can be demonstrated by the massive number of personal "amateur" Web sites which goes to prove that sex can be a means of public expression for some people rather than an individual's or that of a couple. Trying to stop them would be violent breach to freedom of expression.

In the end, a human body isn't something we should shed shame on. It should be an element of pride and if appreciating that pride means showing nude pics of your body to total strangers on the Net, then be it! Who are we to judge them? If it's done right, this can help society as a whole be more relax about the matter and it may be very theraputic for everybody who's at ease with who he or she is.

I hope I didn't take too much of your time and I thank you very much for reading me since I think the future will appeal to each individuals sense of what's right and what is wrong (such as violence, domination, humiliation or abuse).

My best wishes to your work,

--
Claude Gelinas

I am Internet professional. I have been involved in building and deploying Web sites since 1996. I knew then that pornography on the Internet was going to be a problem but I never anticipated that my industry would become a sewer that empties into my own home.

I have two young girls ages 11 and 14. Any child who can spell the word "Dick" or "pussy" can get access to some of the most hard-core content imaginable. Just click, two words above, don't worry, they won't take you to pornographic Web sites but they do take you to a search results page which is one click away from pictures that display hard-core sexual content. And don't kid yourself, that nonsense

> **"This is a site designed and intended SOLELY for ADULTS -- people who are at least 18 years old -- who are interested in and wish to have access to visual images, verbal description and audio sounds of a sexually oriented, frankly erotic nature. ....**
>
> **If you are not accepting all the above Statements, click the link EXIT below or click BACK on your browser now to LEAVE this Adult Site."**

is just that, nonsense. Because for the most part you don't have to click beyond the opening page. There are more often than not pictures on the home pages right in the advertising banners that are so explicit as to show oral and anal sex, animated!!!

I am not naive enough to believe that pornography can be "banned" from the Internet. But asking the smut industry to regulate itself and allow it to hide behind the self-serving disclaimers as to the "adult content" and you are "free to leave the site " warnings is absurd. As is the notion that parental controls in the form of ineffective software filters or "just say no" is an effective means of keeping this out of ones home.

I would be surprised if you're esteemed commission of legal experts, Internet pundits and "freedom of speech" wonks has any real interest in doing what has to be done.

These X-rated storefronts need to be put in their own brown paper bags, if we can hope to protect what little of our children's innocence remains.

Joe Berger

The solution is so easy it is a wonder that it has been overlooked:

Move all the pornography to a new domain called .porn

Credit card the access for age verification and that's the end of it.

As I'm sure you've heard in testimony, biometrics, will be the future of online authentication.
I own a company called Age Protector who has two partners that will allow us to age authenticate on the Internet using a biometric voice sample and Driver License records. This web-based service will allow adult oriented sites to keep minors off, very simply, and across all platforms.

I'd very much like to talk to someone at COPA about this service.
The vendor downloads were specifically about filtering, ISP's and Labeling technologys and don't really apply to this service.

The voice service is up and running and the commerce beta test is going on as we speak.

Who would be a good contact to follow with or submit a vendor proposal?

thanks

Hope the current meeting is going well. Page Howe asked that I pass on to you the overview for .KIDS Domains, Inc that was included in our application to ICANN for a new TLD. We have posted the bulk of our application as well at, http://www.kidstld.com/application/index.htm

I know that Page has had contact with Mr. Telage and we wanted to have this information at your disposal in the event it could be useful in the next 2 days.

Please call me with any questions or if I can be of any assistance.

Matt Hayes
.KIDS Domains, Inc.

It has been stated repeatedly by the government that, they want little involvement with regulating the Internet. While attempting to not interfere in the everyday operations, we find a commendable effort, it is near impossible to not take some sort of role. If individuals and companies (In this case webmasters and surfers) where able to deal with those that "cross lines" or break laws, then we wouldn't need police. Just not going to happen, there will always be those who do a poor attempt of thinking they are beyond whatever rules that are in place. No matter how hard many of us try, we do not have the power or authority to prevent it.

The only downside to Government interaction is many times, they are not fully aware of what they are regulating. The COPA law has many positive attributes but several negative ones as well. There needs to be almost a sub-government working on the Internet as a team to ensure things work smoothly together. In the paragraphs that follow, I will explain who I am followed by what is both strong and week about the current laws. I hope the information will be able to help you with your final report in the later half of October. I apologize for not providing this information sooner, but as you know it takes time to gather information and layout a resolution. If anything needs clarified or re-stated, I will be more then happy to respond and assist any way needed.

My actual name is Steve Dickson, I reside in Indiana and a father of four girls between 5-11 years of age. While working on-line over eight hours a day, I have seen pretty much every aspect of the internet. Everything from <http://www.yahooligans.com/>http://www.yahooligans.com/ which is a great children's search engine, to a site I just reported for child porn. I "talk" to people on the ICQ chat program all the time and have no problem asking them for their impute on any given topic. All this combined has led me to the information to follow

It's been proven time and time again that Child Protection programs (CyberPatrol, NetNanny) are not as effective as the should be. Letting parents depend on these programs alone in negligent. For example, all my children have been on computers for years, my youngest (Age 5) is on our other machine as I type this and has computer lab in school every week. Many parents just don't have the knowledge our children do. I was self taught just like millions of others, I managed to get into computers in the very early 90's so have had a long time to study. Over the years now I have heard things as simple as "How do I find ____ on the internet". I look at the message dumbfounded for a moment then reply "Have you tried a search engine?". Most times they haven't. Now add that to the concerned parent "Protecting their children".

While the government is going to have to make things over complicated so that there are loop-holes (Such as posting nude pictures of children for

adults to spend money to see isn't illegal. As long as it isn't hard-core! That's truly repulsive, but it's "The law") The answers are all very simple.
1. AVS (Adult Verification Systems) Some of these need regulated do to, it can be easy to acquire a password for them. This does tend to be the most viable solution. No content over PG13 without it. Doing so would constitute the violation. This would drastically reduce children's exposure, while focusing on how exactly to help cut down on things like false meta tags (Used in web pages to help search engines index a site)
Example: I did a search for Comicbooks. the third link was nude pictures of Pamela Anderson.

2. It was recently stated in a news article that "It doesn't take a rocket scientist to make current laws work on the internet". 100% correct! Adult Magazines arrive in a black bag or is behind a counter. Adult videos have signs have "Must be 18/21 to enter", this is done on adult web sites, the problem is who is at the counter making sure they at least look old enough?
Think about it for a moment, the site above not only broke the law by exposing the site to children, he used false advertising to do it.
3. It can't be just that simple, it will prove an ineffective as everything else done to date. Major crackdowns have to be made over the entire internet and the best place to start is by working with willing Adult Webmasters and cracking down fast and hard on illegal sites.
Defined: I have a database of over 1100 webmasters, all of which can have an AVS system in place on their sites in less then a week. Many "Mega pay sites" have edited tours and openly promote various AVS services to the webmasters who promote them. I have studied "Partnership programs" from many industries on the internet, the "Adult" programs beat anything else hands down. Better user access, for more detailed and extremely easy to use. While the government allows people to post nude children on the internet, Adult programs are repulsed by it. Free ISP's, affiliate programs and even TGP's (Thumbnail Gallery Posts. 1,000's of hard-core pics for anyone to see updated everyday). Many won't allow over use of the name Lolita, which is the name of a book about a man who "Fell in love" with a 12 year old little girl named Lolita.

It's all really simple to compile together, while complex to maintain to an efficient level.
I. All sites with Content deemed over PG13 must be AVS protected.
a. This includes "Free servers" who have the banner position at the top and bottom of pages.
1. Free servers must provide a "Secured" folder for webmasters to place their protected content. This is very simple process to do, so no one can complain about "resources and time". That's just smoke and mirrors.
2. All webmasters will be able to be properly identified with ease due to they have to give their personal information to the AVS system in order to

be paid
II. Currently non-compliant sites would be fined up to $50,000 per day and up to six months in jail. That's not overly viable "As is"
a. Not all webmasters are on-line everyday; thus, may not get their e-mail everyday. They should receive the first fine just because the did break the law, but should have a "Grace period" before it constitutes a repeat offense.
b. Many webmasters on free servers will never be able to come up with the first $50,000 so forget about any additional.
1. As stated above, the adult industry has the best cgi-scripts for tracking and reporting then any where else on the internet. With this in mind, all should be held accountable. With several programs I have studied, it is VERY possible to track exactly where hits came from for affiliate programs and web servers have total access to things on their servers.
c. The webmaster is the single largest entity responsible for the content they post and where. They should receive the full amount of any jail time issued. In addition, there will be records of how much they have earned and that will estimate how much of the fines they should pay.
1. The servers be it a free or paid hosting is aware of how many hits a site gets and to what pages, they have the ability to terminate any account with ease. I see no reason why they can't police sites for wrongful activities.
2. Affiliate programs also have full access to where hits come from. It is far more difficult for them to regulate due to webmasters are on many different servers. Most of those servers are not regulated by them and they would have to contact both the offending webmasters and the server they are hosted on.
3. Many webmasters will quickly become compliant upon receiving the knowledge that they can and will be charged. The servers should be the primary target for cash fines, and affiliate programs to a lesser degree. None can complain about "Additional costs" of operating. Most brick and motor stores have loss prevention, expensive surveillance equipment and other things to do similar jobs. While it will be more costly for affiliates to regulate that many webmasters, they almost all have the same clause. Violate the terms of service and the account is canceled without payment. That
could be nothing or in some cases $1000.00's.
d. There are a good number of webmasters who would like to be more compliant, but thanks to no law enforcement of any kind, it is difficult for them to do so and still "compete" It's easy to just blame one sector of a problem, but that is both unfair and not effective.
1. The Adult industry as a whole can be compliant and strive to obey the laws and it will do a lot of good. They can't do it alone. What is needed is a central location for the adult industry to help each other. This happens all the time, I can provide countless links to web sites ran by multiple sites for a common reason. If sites, surfers, webmasters and such could log in and

provide violators web address then, many sites could ease the strain of finding them all.
2. There are plenty of "outside" factors that will effect the efficiency of any law. The current joke with Napster is a prime example. Many servers won't allow "Complete" MP3 files. Affiliate programs like Amazon.com will cancel an account if they discover a site makes complete songs available. ITS THEFT. There is the argument that people have been sharing files with friends for years. Very true! None of us have ever shared them with 30 million of our "Closest friends". If Napster isn't shut down, then why not make Warez legal? If you can steal music, steal programs. That leaves the door open for password trader sites, which is stealing services and directly allows children to get passwords to porn sites.
3. Mistakes happen, with any medium, so should not be treated in an over zealous fashion. A blind link. tricks a person from leaving where they are in order to go to a site they had little or no interest in. Upon reading documentation on false advertising, you will see this fills many of the "requirements".
<http://www.lawnotes.com/false_advertising.htm>http://www.lawnotes.com/false_advertising.htm
4. Hacking a computer requires entering a home or business threw the phone lines and proceeding to read or destroy private property.
<http://www4.law.cornell.edu/uscode/18/1030.html>http://www4.law.cornell.edu/uscode/18/1030.html
5. The Internet is like no other technology in the history of mankind. The United States Government should be in charge of all laws governing the Internet in the United States. Allowing individual states to regulate them selves while have the sovereignty of the union is a great factor in what has propelled our country to where it is today.
There are federal laws that supersede the individual states and this should be true in dealing with the internet. More work, complicated laws and other things can be avoided if there is only one version of a law. Gambling, Adult content, taxes or anything else.
Example: Texas banned Ford from selling used cars on-line to consumers. The car want to retailers in the area and all inspections and taxes had to be paid. I would be upset if the congress from Indiana pulled such a stunt.
6. The standing law in regards to "Adult content" while using children needs revised.
<http://www4.law.cornell.edu/uscode/18/2256.html>http://www4.law.cornell.edu/uscode/18/2256.html Just paying by credit card to see nude children, "Hardcore" or not, should send up red flags.
7. Credit Card companies are multi-billion dollor ego maniacs. Their sole concern is making money, with little to no regard for their clients. They impose stiff fines for excessive charge backs. The leading industry for this is Adult Websites because a portion of consumers find it easy to do. IBill and others have software installed to detect card numbers that make a habit of charging back and refuse to except them with their clients. Credit

Card Companies should be forced to use similar software, fine the companies that are at fault, but repeated service thiefs shouldn't be allowed to "refund" every other day. There is a lot less profit not fining innosent companies so to date have no interest in being honest about it.

Without all of the above working together any individual law will be substantially less effective then it could be. There are of course much more in-depth factors, but they are impossible to portray is a single e-mail. As stated in the opening lines of this message, Myself and many others are more than willing to contribute in anyway we can. We do not represent any one company or industry, so can remain neutral, while wanting to protect children and the rights of legal adults. A great deal of us understand the workings of the internet, but more importantly can provide the perspective of what "Actually" goes on around the internet.

Sincerely,
Steven G. Dickson

Dear sir of madam,

Thank goodness for your committee. I support restrictions on children's access to porn on the Internet.

I have a method that will help reduce access by minors to material that is harmful to minors on the Internet. Maybe we should make computers cost more than $200. I can't think of any kid that has $200 for a computer so this would keep most of the kids off the net.

Or the children could impldment "parent" version 1.0. This is a program that is rarely used these days and once activated would rid children from viewing material that is harmful to minors on the Internet. It appears that most the "parent" programs are still in beta and require millions of plug-ins to keep children from viewing material that is harmful to minors on the Internet. It seems easier to fix the ONE "parent" program than it is to fix the MILLIONS of plug-ins to rid children from viewing material that is harmful to minors on the Internet.

I was just reading a news report about more police on the web has any thought been given to retired P.O. I am a retired New York City Police Office that has time to spend on the web you could make these retired officer marshal and you could have a lot of experience to help in this fight

it just a idea but with some merit I think

Craig V Hewitt

In the report, the commission cautioned that governments need to "pay competitive salaries and benefits" to retain Web-savvy cops in an era where technical skills command high dollars.

Since it sounds like high paid web savvy cops are wanted, why not hire a minimum number of cops to serf the net for child porno and let them check up on sites which are turned in by ordinary web serfers who are paid rewards when a conviction occurs. This seems to me to be a more cost effective way to spend money for salaries.

Thank you,
Gerald Erikson

Compilation of Matrices on Filtering, Labeling, and Rating Technologies

The COPA Commission created a questionnaire to compile information on the existing filtering, labeling and rating technologies that are available in the marketplace. The questionnaire was widely distributed to a broad range of companies, including organizations listed in the GetNetWise Internet Safety Tools directory, visitors to the COPA Commission web site, and to anyone who requested a copy from the Commission. Commissioners and their staff were also encouraged to distribute the questionnaire to their contacts. The responses are presented in a matrix format that allows for a question-by-question comparison of the products.

Compilation Matrix Acrobat PDF file, 256Kb, 136 pages in landscape, letter size paper

---

webmaster@copacommission.org / Copyright © 2000

BEST COPY AVAILABLE

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling and Rating Technologies

	Anti-Defamation League Hatefilter (ADL) Anti-Defamation League Hatefilter 823 United Nations Plaza New York, NY 10017	**Awesome Library Website (EDI)** Evaluation & Development Institute 100 Kerr Parkway, #39 Lake Oswego, OR 97035
Narrative Product Description	Anti-Defamation League Hatefilter protects children by blocking access to World Wide Web sites of individuals or groups that, in the judgment of ADL, advocate hatred, bigotry, or even violence towards Jews or other groups on the basis of their religion, race, ethnicity, sexual orientation, or other immutable characteristics. **(See Anti-Defamation League Hatefilter (ADL) 1.3)**	Awesome Library organizes the Web with 14,000 carefully reviewed resources, including the top five % in education. Resources are "child-safe". **(See Awesome Library 1.3)**
A. GENERAL QUESTIONS		
1 Select which best describes your product or service		
a Filtering ISP		
b Client Side Filter	P	
c Filtered search engine		P
d Filtered browser		P

BEST COPY AVAILABLE

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling and Rating Technologies

	BASCOM Global Internet Services, Inc. 275 Marcus Blvd. Suite R Hauppauge, NY 11788	**Chaperon 2000** ComerPost Software PO Box 405 Duffied, VA 24263
Narrative Product Description	BASCOM is a software development company specializing in Linux-based thin server and content management applications Since its inception, BASCOM has made next generation security, connectivity and content management technology available for small to mid-sized networks and K-12 Schools, offering a pioneering approach to simple, affordable, low-maintenance deployment. **(See BASOM 1.3)**	**This questionnaire is predisposed to the belief that all solutions to inappropriate Internet material have been identified. The approach that we are presenting is not one of these identified methods. Thus the profile of our approach to this problem generated by this matrix will be flawed. Please include the attached paper on Chaperon in your evaluation to our solution. (See Chaperon)** Our product filters, however it compensates for filter's shortcomings by notifying administrators of possible filter issues. This brings humans into the loop allowing a human to make the appropriate/inappropriate material decision instead of leaving it up to a computer. **(See Chaperon 2000 1.3)**
A. GENERAL QUESTIONS		
1. Select which best describes your product or service		
a. Filtering ISP		
b. Client Side Filter	P	
c. Filtered search engine		
d. Filtered browser	P	

	Characterlink	**Childwatch by PACEL Corporation**
Narrative Product Description	We filter the Internet using a white-list, server based system. Customers submit sites, then we attribute the site. Customers then choose what attributes they want blocked. **(See Characterlink 1.3)**	Childwatch allows parents to control and monitor their children's activities on the computer. In addition, a filtering service prevents access to pornography on the Internet. The software also displays through a screen saver pictures of missing and exploited children provided by Child Watch of North America, Inc. **(See Childwatch 1.3)**
A. GENERAL QUESTIONS		
1. Select which best describes your product or service		
a. Filtering ISP	P	
b. Client Side Filter		P
c. Filtered search engine		
d. Filtered browser		

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling and Rating Technologies

	Cyber Patrol 1900 West Park Drive, Suite 180 Westborough, MA 01581	**Cyber Sentinel V2.0** Security Software Systems 1998 Bucktail Ln Sugar Grove, IL 60554
Narrative Product Description	Cyber Patrol is Internet filtering software. It is used in homes, schools, libraries, and businesses to prevent access to inappropriate content. **(See Cyber Patrol 1.3)**	Cyber Sentinel V2.0 is an advanced Internet filtering software package, it provides a unique proactive model for analyzing, monitoring, filtering, and blocking predatory, pornographic, and sexually explicit computer traffic. In addition it is the only product to provide real=time protection for children from predators and pedophiles in all chat rooms, instant messaging, e-mail and e-mail attachments. A data collection feature allows parents, administrators and law enforcement to review inappropriate and potentially harmful material gathered from the computer. Cyber Sentinel also has built-in time management so you can control during what hours users have access to the world wide web, e-mail, newsgroups and more. **(See Cyber Sentinel and Cyber Sentinel 1.3.)**
A. GENERAL QUESTIONS		
1. Select which best describes your product or service		
a. Filtering ISP		
b. Client Side Filter	P	P
c. Filtered search engine		
d. Filtered browser		

BEST COPY AVAILABLE

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling and Rating Technologies

	CYBERsitter 2000 Solid Oak Software, Inc PO Box 6826 Santa Barbara, CA 93160 (805) 884-8201	**Desktop Surveillance** Tech Assist, Inc 18830 U S 19 N, Suite 323 Clearwater, FL 33764
Narrative Product Description	CYBERsitter, the original Internet filter, is an easy to use software program that protects children by filtering inappropriate Internet content and comes with over 30 different filters in numerous categories including adult, violence, hate related, and even those annoying popup ads. Simply select the categories you want to restrict access to, and CYBERsitter will keep your filters updated automatically at no additional cost as well as maintain a complete history of all Internet activity and provide privacy and time controls	Desktop Surveillance records both visually and in text, any or all desktop computer usage including but not limited to the Internet. It also features key word access control. **(See Desktop Surveillance 1.3)**
A. GENERAL QUESTIONS		
1. Select which best describes your product or service		
a. Filtering ISP		P
b. Client Side Filter	P	P
c. Filtered search engine		P
d. Filtered browser		P

	Digimarc Corporation 19801 SW 72nd Ave., Ste 250 Tualatin, OR 97062 503-885-9699	**Dotsafe, Inc.** 8181 South 48th St. #120 Phoenix, AZ 85044
Narrative Product Description	Digimarc patented digital watermarking solutions embed imperceptible information within images. Digimarc has - in an attempt to make the Internet a safer place for children - offered to license its watermark reading technology to filtering and browser vendors at no charge to help filter unwanted adult content on the Web and has offered to provide content distributors with a unique ID - that Digimarc will make publicly available - to easily embed Adult Flag watermarks in images that may be potentially harmful to children. Digimarc's watermark reading technology can be integrated by browser and filtering applications to detect and filter images watermarked with an Adult Flag, according to user preferences. The Adult Flag can be embedded in images using one of the millions of copies of Digimarc-enabled imaging tools that they are already in the market and are widely used to prepare images for the Web (including applications from leading vendors of digital imaging and asset management applications like Adobe, Corel, Cerious Saftware, CreativePro, Datamark, Equilibrium, Jasc Software, Micrografx, TrueSpectra, Ulead, and Xat.com) **(See Digimarc 1.3. Also see Digimarc Other)**	Dotsafe provides Internet and email filtering products for enterprise and individual use. Dotsafe's products are designed for the Education, Consumer, and Business markets.
A. GENERAL QUESTIONS		
1. Select which best describes your product or service		
a. Filtering ISP	P	
b. Client Side Filter	P	
c. Filtered search engine	P	
d. Filtered browser	P	P

759

Commission on Online Child Protection (Filtering Evaluation)
Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling, and Rating Technologies

	E-Junk, Obvious Solutions c/o Obvious Solutions, 500 Summer St, Suite 404 Stamford CT 06901	**FamilyClick.com, LLC** 2877 Guardian Lane, Suite 300 Virginia Beach, VA 23452	**FamilyConnect** **S4F Technologies** 2448 E 91st St, Suite 3300 Tulsa OK 74137
Narrative Product Description	E-Junk filters junk and offensive e-mail under control of a local administrator	FamilyClick is a family oriented filtered internet service provider and portal with fully comprehensive, family suitable content. Our service offers multiple levels of access geared to different age groups, five e-mail addresses that filter out spam and offensive language, personal web space, and controls for instant messaging, chat, and newsgroups. **(See FamilyClick 1.3)**	FamilyConnect provides filtered Internet access.
A. GENERAL QUESTIONS			
1. Select which best describes your product or service			
a. Filtering ISP		P	P
b. Client Side Filter	P		
c. Filtered search engine			
d. Filtered browser			

	iForAll **Developed by InForAll, Inc.** 12200 Tech Rd #303 Silver Spring, MD 20904	**Integrity Online**	**Integrity Online of Wichita Falls, TX DBA** SHAMMER.com 3815 McNiel, Wichita Falls, TX 76308
Narrative Product Description	iForAll allows real-time monitoring, blocking, filtering and communications between parents and children's computer's). iForAll connects parents and children's computers together from anywhere in the world and allows parents to participate in their child's online experience.	Filters known URLs that contain inappropriate material such as pornography.	Filtered ISP blocks porn and objectionable material.
A. GENERAL QUESTIONS			
1. Select which best describes your product or service			
a. Filtering ISP		P	
b. Client Side Filter	P		
c. Filtered search engine			
d. Filtered browser			

Commission on Online Child Protection (Filtering Evaluation)
Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling and Rating Technologies

	Internet Safari, by Heartsoft, Inc. 3101 N Hemlock Circle Broken Arrow, OK 74014	**ITECH INC.** 6601 Washington Avenue Racine, WI 53406
Narrative Product Description	Internet Safari is a secure children's browser. **Internet Safari incorporates five types of filtering in six categories into a proprietary children's browser. Each category for filtering will have** adjustable tolerance levels. **(See Internet Safari 1.3)**	IWAYPATROL-Internet Filtering for Schools; **CHILDREN'S DEPT-Internet Filtering** for Libraries; **ISPFAMILYFILTER**-Internet Filtering for ISPs; GBTW-2000- Internet Filtering for Offices; SAFEMAIL- Filtering for email for Schools. iTech provides Internet Content Filtering for a variety of settings, including schools and libraries. It is a server-based filter that is based on local controls of all parameters. It offers multiple filtering approaches (list based, labels, content) and age differential filtering.
A. GENERAL QUESTIONS		
1. Select which best describes your product or service		Server based filter -- unless I am missing something? We wouldn't normally call what we do a filtered search engine or a filtered
a. Filtering ISP		
b. Client Side Filter		
c. Filtered search engine		
d. Filtered browser	P	

	Microsoft IE5 Content Advisor **Netscape Communicator 4.7 Netwatch** **(c/o RSACi)**
Narrative Product Description	**All information is provided by Internet Content Rating Association** Filtering services allows parents and other concerned adults the means to filter material from the Internet they judge is inappropriate for their children. Both Microsoft's Content Advisor and Netscape's Netwatch read the RSACi html labels written in the PICS language and provide or deny access according to the levels set by a parent. There is an option to block unrated sites and an option to add sites into an Approved List. **(See MSIE5 1.3)**
A. GENERAL QUESTIONS	
1. Select which best describes your product or service	
a. Filtering ISP	
b. Client Side Filter	
c. Filtered search engine	
d. Filtered browser	P

	N2H2
Narrative Product Description	Provides complete turnkey server based filtering systems for its customers. N2H2 provides the hardware, the proprietary software, and the continuous review and filter list updates that are required to keep the system up-to-date and accurate. N2H2 does not make decisions as to what type of Internet content is or is not appropriate; instead, N2H2 categorizes content and allows its customers to decide what is appropriate for their networks or computers. **(See Net Nanny 1.3)**
A. GENERAL QUESTIONS	
1. Select which best describes your product or service	
a. Filtering ISP	N2H2 is an ASP for over 200 ISPs and VISPs. Although N2H2 does not and will not provide what has traditionally been considered a client side filter, N2H2 will soon be shipping software that can be installed on a home computer that will allow a parent to configure specific filter policies for different members of their family. Unlike traditional client filtering software, however, the URL list is maintained on a server hosted at their ISP and will not have to be maintained/ updated on the home computer. Is our award winning searchopolis.com
b. Client Side Filter	
c. Filtered search engine	
d. Filtered browser	

BEST COPY AVAILABLE

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling, and Rating Technologies

	Net Nanny Software, Inc. 15831 NE 8th, Suite 200 Bellevue, WA 98008	**PlanetGood Technologies, Inc.** (formerly BrowseSafe.com) 7202 E. 87th St. Suite 109 Indianapolis, IN 46256
Narrative Product Description	Net Nanny 3.1 filters, monitors and /or blocks Web sites, chat, newsgroups and instant messaging content according to the individual needs and values of the family and/or organization that uses it. All of its lists of words, phrases and sites are completely viewable and editable by the administrator of the software. Administrators can choose to block access, send warning messages, log activity and/or mask incoming and outgoing words and phrases, including personal information. **(See Net Nanny 1.3)**	PlanetGood is an internet experience provider, a smart filter, that allows browsing of the Internet through sites that have been reviewed by human eyes. Each site is categorized according to a set of 37 characteristics, and access to sites containing those characteristics is determined by parents. By reviewing every link of every site, PlanetGood allows all of the good information to be accessed and all of the bad is not able to be viewed. **(See PlanetGood 1.3)**
A. GENERAL QUESTIONS		
1. Select which best describes your product or service		
a. Filtering ISP		
b. Client Side Filter	P	P
c. Filtered search engine		
d. Filtered browser		

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling and Rating Technologies

	REALTIME SENTRY Dr. Gregory R. Jackson, Pres/CEO eplacetogo, inc 1117 South 22nd St Birmingham, AL 35205	**RSACi, Internet Content Rating Services/ Products** 3460 Olney-Laytonsville Road, Suite 202 Olney, MD 20832 AND ICRA, 22old Steine, Brighton BN1 1EL, UK
Narrative Product Description	REALTIME SENTRY, empowered by **CONTEXION technology**, is a proven, real-time content analyzer that efficiently and accurately identifies inappropriate content of web pages. It combines atomization of a web page with text analysis, image analysis, and site analysis at sub-second speed. Unlike list-based filters, this dynamic approach assures that even brand new or changed web pages are accurately analyzed. REALTIME SENTRY uses proprietary client-side software, network servers, and CONTEXION technology to offer seamless, real-time and powerful protection from the explosive growth of the smut of the Internet	The RSACi labeling facility allows content authors to appropriately label their content online according to a set classification schema. It further allows parents and care givers the facility to filter access to Internet content through their PCs according to their views on protecting minors using the Internet. **(See RSACi 1.3)**
A. GENERAL QUESTIONS		
1. Select which best describes your product or service		
a. Filtering ISP		
b. Client Side Filter		
c. Filtered search engine		
d. Filtered browser		P

	Safe Access PO Box 2757 Flagstaff, AZ 86003	**SafeSurf Internet Filtering Solution**
Narrative Product Description	Safe Access is a filtered ISP service, blocking out unwanted material (pornography, criminal skills, illegal drug use) for its customers using "server-side" technology. **1.3 Documentation request**: Safe Access blocks out web sites that fall within the following categories:Y9 Criminal Skills, Cults, Drugs, Obsene & Tasteless, Public Proxies, Pornography, Hate Groups	The SafeSurf Internet Filtering Solution enables the creation and maintenance of family oriented portals and search engines.
A. GENERAL QUESTIONS		
1. Select which best describes your product or service		
a. Filtering ISP	P	
b. Client Side Filter		
c. Filtered search engine		P
d. Filtered browser		P

Commission on Online Child Protection (Filtering Evaluation)
Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling, and Rating Technologies

	Safexplorer 700 - 509 Richards St Vancouver, BC Canada V65 2Z6	**Stanford University**	**WinGuardian** PO Box 3531 Boulder, CO 80307
Narrative Product Description	A multi-user browser incorporating numerous security methods including rating. Parents are empowered to customize the program and choose the categories and vocabulary they wish to filter. **(See Safexplorer)**	No product, only a technology for others.	WinGuardian is a monitoring utility and filtering alternative. WinGuardian can keep track of what programs a user runs, log any text that is typed into a program, log all web sites that are visited, and even capture screen shots at various specified intervals. This can provide parents and teachers with the information they need to start conversations with children regarding responsible use of the Internet.
A. GENERAL QUESTIONS			
1. Select which best describes your product or service			
a. Filtering ISP			
b. Client Side Filter			P
c. Filtered search engine			
d. Filtered browser	P		

	XSTOP.com R2000 www.xstop.com	**Yahoo!** Dittus Communications 3420 Central Expressway Santa Clara, CA 95051
Narrative Product Description	X-STOP provides server based filtering technology to allow ISPs to provide Internet filtering service to families, education, and businesses. X-STOP R2000 technology builds with high capacity filtering engine and doesn't degrade network performance. **(See XSTOP 1.3)**	While Yahoo! does not have one specific "filtering" product, several products include technology or manual processes that in effect "filter" for content and/or language. In particular, Yahooligans! http://www.yahooligans.com/ is a manually created directory of websites and content selected especially children ages 7 - 12. Yahoo! Mail http://mail.yahoo.com/ and Messenger http://messenger.yahoo.com/ offer users the choice of filtering who communicates with them. Geocities http://geocities.yahoo.com/home/ uses filters to prohibit website searches for content inappropriate for children.
A. GENERAL QUESTIONS		
1. Select which best describes your product or service		
a. Filtering ISP	PWe are technology provider	
b. Client Side Filter	P	
c. Filtered search engine		Yahooligans! Is a directory of websites for children ages 7-12. Because the sites are selected individually by editors, all searches are by default "filtered". This is NOT a technology, but rather a result of the human editorial process.
d. Filtered browser		

	Zeek Safe (Zeeks.com, Inc.) 5200 SW Macadam Ave, Suite 570 Portland, OR 97201
Narrative Product Description	Zeek Safe is a free Internet filter that restricts access by children to over 350,000 inappropriate adult web sites. Zeek Safe allows parents to add/remove sites from the blocked list, set word filters, and set browsing hours. **(See Zeek Safe 1.3)**
A. GENERAL QUESTIONS	
1 Select which best describes your product or service	
a. Filtering ISP	
b. Client Side Filter	P
c. Filtered search engine	
d. Filtered browser	

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling, and Rating Technologies

	Anti-Defamation League Hatefilter (ADL)	Awesome Library Website (EDI)
2 Product or service works with the following operating systems (Check all appropriate)		
a Windows 3.1	P	
b Windows 95	P	
c Windows 98	P	
d Windows 2000		
e Windows NT	P	
f MacOS		
g Other		P Unix, Browsers
3 Filters block access to the following (check all appropriate)		
a Sexually explicit material		P
b Graphic violence		P
c Hate groups	P	P
d Illegal activity		P
e On-line gambling		P
f Personals		P
g Occult		P
h Web based e-mail		
i Free ISPs		
j Other		
4 For the categories selected in number 3, do your filters (check all appropriate)		
a Filter outgoing messages and search requests		
Filter incoming messages and search results		P
5 How many levels of filtered access do you offer?		
a 1	P	P
b 2		
c 3		
d 4		
e 5		
f More than 5		

782

783

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling, and Rating Technologies

	BASCOM Global Internet	Chaperon 2000
2 Product or service works with the following operating systems (Check all appropriate)		
a Windows 3.1	P	
b Windows 95	P	
c Windows 98	P	
d Windows 2000	P	
e Windows NT	P	
f MacOS	P	
g Other		
3 Filters block access to the following (check all appropriate):		
a Sexually explicit material	P	
b Graphic violence	P	
c Hate groups	P	
d Illegal activity	P	
e On-line gambling	P	
f Personals	P	
g Occult	P	
h Web based e-mail	P	
i Free ISPs	P	
j Other		
4 For the categories selected in number 3, do your filters (check all appropriate)		
a Filter outgoing messages and search requests	P	WE check for notification purposes, but do not
Filter incoming messages and search results	P	
5 How many levels of filtered access do you offer?		
a 1		
b 2		
c 3		
d 4	P	
e 5		
f More than 5		

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering Labeling and Rating Technologies

	Characterlink	**Childwatch by PACEL Corporation**
2 Product or service works with the following operating systems (Check all appropriate)		
a Windows 3 1	P	
b Windows 95	P	P
c Windows 98	P	P
d Windows 2000	P	
e Windows NT	P	
f MacOS	P	
g Other		
3 Filters block access to the following (check all appropriate)		
a Sexually explicit material	P	P
b Graphic violence	P	
c Hate groups	Administrators of the accounts can choose to	
d Illegal activity	P	
e On-line gambling	P	
f Personals	Administrators of the accounts can choose to	
g Occult	P	
h Web based e-mail	Administrators of the accounts can choose to block these or leave them open	
i Free ISPs		
j Other		
4 For the categories selected in number 3, do your filters (check all appropriate)		
a Filter outgoing messages and search requests		
Filter incoming messages and search results	P	P
5 How many levels of filtered access do you offer?		
a 1		P
b 2	P	
c 3		
d 4		
e 5		
f More than 5		

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling and Rating Technologies

	Cyber Patrol	Cyber Sentinel V2.0
2. Product or service works with the following operating systems (Check all appropriate)		
a. Windows 3.1	P	P
b. Windows 95	P	P
c. Windows 98	P	P
d. Windows 2000	P	P
e. Windows NT	P	P
f. MacOS	P	
g. Other		
3. Filters block access to the following (check all appropriate):		
a. Sexually explicit material	P	P
b. Graphic violence	P	
c. Hate groups	P	
d. Illegal activity	P	
e. On-line gambling	P	
f. Personals	P	
g. Occult		
h. Web based e-mail	P	
I. Free ISPs	P	
j. Other		P
4. For the categories selected in number 3, do your filters (check all appropriate)		
a. Filter outgoing messages and search requests	P	P
Filter incoming messages and search results	Web filtering	P
5. How many levels of filtered access do you offer?		
a. 1		
b. 2		
c. 3		P
d. 4		
e. 5		
f. More than 5	Customizable	

788

789

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling, and Rating Technologies

	CYBERsitter 2000	Desktop Surveillance
2. Product or service works with the following operating systems (Check all appropriate)		
a. Windows 3.1		
b. Windows 95	P	P
c. Windows 98	P	P
d. Windows 2000	P	P
e. Windows NT	P	P
f. MacOS		
g. Other	P + ME	
3. Filters block access to the following (check all appropriate)		
a. Sexually explicit material	P	P
b. Graphic violence	P	P
c. Hate groups	P	P
d. Illegal activity	P	P
e. On-line gambling	P	P
f. Personals	P	P
g. Occult	P	P
h. Web based e-mail	P	P
i. Free ISPs		P
j. Other	P + 21 Additional Categories	P
4. For the categories selected in number 3, do your filters (check all appropriate)		
a. Filter outgoing messages and search requests	P	P
Filter incoming messages and search results	P	N/A
5. How many levels of filtered access do you offer?		
a. 1	P	
b. 2		
c. 3		
d. 4		
e. 5		
f. More than 5		

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling and Rating Technologies

	Digimarc Corporation	Dotsafe, Inc.
2 Product or service works with the following operating systems (Check all appropriate)		
a Windows 3.1		P
b Windows 95	P	P
c Windows 98	P	P
d Windows 2000	P	P
e Windows NT	P	P
f MacOS	P	P
g Other		
3 Filters block access to the following (check all appropriate):	Any image watermarked with the Adult Flag, including A & B: Hate Groups; Illegal activity; On-line gambling; Personals; Occult; Web based email; Free ISPs; Other	
a Sexually explicit material	P	P
b Graphic violence	P	P
c Hate groups	P	P
d Illegal activity	P	P
e On-line gambling	P	P
f Personals	P	P
g Occult	P	P
h Web based e-mail	P	P
i Free ISPs	P	P
j Other	P	P
4 For the categories selected in number 3, do your filters (check all appropriate)		
a Filter outgoing messages and search requests		P
Filter incoming messages and search results	P	P
5 How many levels of filtered access do you offer?	One level of filtering is available today through the Adult Content Flag, but we could offer additional bits in future versions of this solution.	
a 1	P	P
b 2		
c 3		
d 4		
e 5		
f More than 5	P	Available 1/1/01

792

793

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling and Rating Technologies

	E-Junk, Obvious Solutions	FamilyClick.com, LLC	FamilyConnect
2. Product or service works with the following operating systems (Check all appropriate)			
a. Windows 3.1			
b. Windows 95		P	P
c. Windows 98		P	P
d. Windows 2000			P
e. Windows NT			P
f. MacOS		P	
g. Other	P		Windows ME
3. Filters block access to the following (check all appropriate).			
a. Sexually explicit material	P	P	P
b. Graphic violence		P	
c. Hate groups		P	P
d. Illegal activity		P	P
e. On-line gambling		P	
f. Personals		P	
g. Occult		P	
h. Web based e-mail		P	
i. Free ISPs			
j. Other	P	P	
4. For the categories selected in number 3, do your filters (check all appropriate)			
a. Filter outgoing messages and search requests		P	P
Filter incoming messages and search results	P	P	
5. How many levels of filtered access do you offer?			
a. 1			
b. 2	P		P
c. 3			
d. 4			
e. 5		P	
f. More than 5			

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling, and Rating Technologies

	iForAll	Integrity Online	Integrity Online
2. Product or service works with the following operating systems (Check all appropriate)			
a. Windows 3.1		P	
b. Windows 95		P	
c. Windows 98	P	P	
d. Windows 2000		P	
e. Windows NT	P	P	
f. MacOS		P	
g. Other			
3. Filters block access to the following (check all appropriate)			
a. Sexually explicit material	P	P	P
b. Graphic violence	P	P	P
c. Hate groups	P	P	P
d. Illegal activity	P	P	P
e. On-line gambling	P	P	P
f. Personals	P	P	
g. Occult	P	P	P
h. Web based e-mail	P		
i. Free ISPs	P	P	P
j. Other	P		P
4. For the categories selected in number 3, do your filters (check all appropriate)			
a. Filter outgoing messages and search requests	P	P	
Filter incoming messages and search results	P		P
5. How many levels of filtered access do you offer?			
a. 1	P	P	P
b. 2			
c. 3			
d. 4			
e. 5			
f. More than 5			

796

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling, and Rating Technologies

	Internet Safari, by	ITECH INC.
2. Product or service works with the following operating systems (Check all appropriate)		
a. Windows 3.1	P	P
b. Windows 95	P	P
c. Windows 98	P	P
d. Windows 2000	P	P
e. Windows NT	P	P
f. MacOS	P	P
g. Other		We have a server-based filter that actually runs on any Unix server. In terms of the question as worded, the IWAYPATROL filter works on any workstation that can run any browser using any kind of operation system including Solaris, Linux, Freebsd, Etc.
3. Filters block access to the following (check all appropriate)	Image Filtering - Graphic Image Analysis	
a. Sexually explicit material	P	P
b. Graphic violence	P	P
c. Hate groups	P	P
d. Illegal activity		P
e. On-line gambling		P
f. Personals		P
g. Occult	P	P
h. Web based e-mail	P html based provided with browser	P
i. Free ISPs		
j. Other	Behavior (Gangs, attacks, etc.), Drugs, Nudity, Profanity	Drugs, gun sales, chat, alcohol, tobacco, language, adult password and access sites. Optional and under local control.
4. For the categories selected in number 3, do your filters (check all appropriate)		
a. Filter outgoing messages and search requests	P	P
Filter incoming messages and search results	P	P
5. How many levels of filtered access do you offer?		There is no question in your matrix related to age-level filtering, but we offer the option of filtering by age group or grade as well as by
a. 1		
b. 2		
c. 3		
d. 4		
e. 5		
f. More than 5	P	P

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling and Rating Technologies

	Microsoft IE5 Content Advisor
2. Product or service works with the following operating systems (Check all appropriate)	
a. Windows 3.1	
b. Windows 95	P
c. Windows 98	P
d. Windows 2000	P
e. Windows NT	P
f. MacOS	P
g. Other	
3. Filters block access to the following (check all appropriate):	
a. Sexually explicit material	P
b. Graphic violence	P
c. Hate groups	P
d. Illegal activity	
e. On-line gambling	
f. Personals	
g. Occult	
h. Web based e-mail	
i. Free ISPs	
j. Other	P
4. For the categories selected in number 3, do your filters (check all appropriate)	
a. Filter outgoing messages and search requests	
Filter incoming messages and search results	
5. How many levels of filtered access do you offer?	
a. 1	
b. 2	
c. 3	
d. 4	
e. 5	
f. More than 5	P

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling and Rating Technologies

	N2H2
2. Product or service works with the following operating systems (Check all appropriate)	
a. Windows 3.1	P
b. Windows 95	P
c. Windows 98	P
d. Windows 2000	P
e. Windows NT	P
f. MacOS	P
g. Other	All of the above. All operating systems and browsers are supported since there is no requirements to install client software
3. Filters block access to the following (check all appropriate)	
a. Sexually explicit material	P
b. Graphic violence	P
c. Hate groups	P
d. Illegal activity	P
e. On-line gambling	P
f. Personals	P [Free WebPages hosts]
g. Occult	P
h. Web based e-mail	P
I. Free ISPs	P
j. Other	Nudity/Language P
4. For the categories selected in number 3, do your filters (check all appropriate)	
a. Filter outgoing messages and search requests	P
Filter incoming messages and search results	
5. How many levels of filtered access do you offer?	
a. 1	
b. 2	
c. 3	
d. 4	
e. 5	
f. More than 5	P All categories can be on or off resulting in hundreds of possible configurations.

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling, and Rating Technologies

	Net Nanny Software, Inc.	PlanetGood Technologies, Inc.
2. Product or service works with the following operating systems (Check all appropriate)		
a. Windows 3.1	P	
b. Windows 95	P	P
c. Windows 98	P	P
d. Windows 2000		P
e. Windows NT		P
f. MacOS		
g. Other		
3. Filters block access to the following (check all appropriate)		
a. Sexually explicit material	P	P
b. Graphic violence	P	P
c. Hate groups	P If user inputs sites	
d. Illegal activity	P If user inputs sites	
e. On-line gambling	P	P
f. Personals	P If user inputs sites	
g. Occult	P	P
h. Web based e-mail	P	
i. Free ISPs		
j. Other	Yes - Users can include any other types of sites that they wish to block. Kids may be spending too much time playing games or accessing sites that distract them from school work. Sites may not be generally viewed as inappropriate, but it is the parent's prerogative to decide what should or shouldn't be blocked.	PlanetGood rates according to 37 characteristics which are: alcohol, alternative lifestyles, Art-Nudity, Extreme Beach, Intimate Apparel, Chat, Message Boards/clubs, New Age/Eastern Religions, Gambling, Games, Illegal Drugs, Hunting & Firearms, Jokes/Humor, Non-technical Downloads, Mature Subject Matter, Mature Sexual Language, Medical Nudity, Medical Sexual Terminology, Movies/TV, Music, News, Occult Sites, Online ordering, Paranormal, Pop Culture, Science Fiction, Personal Web Pages, Pornography, Profanity Excessive, Profanity Mild, Reviews/Critics, Search Engines, Sports, Tobacco, Video or Audio, Violence, Violence Moderate, and Violence Excessive.
4. For the categories selected in number 3, do your filters (check all appropriate)		
a. Filter outgoing messages and search requests	P	P
Filter incoming messages and search results	P	P
5. How many levels of filtered access do you offer?	Not clear on what question means	
a. 1		
b. 2		
c. 3		
d. 4		
e. 5		
f. More than 5		P 37 exactly

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling and Rating Technologies

	REALTIME SENTRY	RSACi, Internet Content Rating Services/
2. Product or service works with the following operating systems (Check all appropriate)		
a. Windows 3.1		
b. Windows 95	P	P
c. Windows 98	P	P
d. Windows 2000		P
e. Windows NT		P
f. MacOS		P
g. Other		
3. Filters block access to the following (check all appropriate):		
a. Sexually explicit material	P	P
b. Graphic violence	P	P
c. Hate groups	P	P
d. Illegal activity	P	
e. On-line gambling		
f. Personals		
g. Occult		
h. Web based e-mail	P	
i. Free ISPs		
j. Other		Nudity/Language
4. For the categories selected in number 3, do your filters (check all appropriate)		
a. Filter outgoing messages and search requests	P	
Filter incoming messages and search results	P	
5. How many levels of filtered access do you offer?		
a. 1	Complete real-time content analyzer	
b. 2		
c. 3		
d. 4		
e. 5		
f. More than 5		P

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling and Rating Technologies

	Safe Access	SafeSurf Internet Filtering Solution
2. Product or service works with the following operating systems (Check all appropriate)		
a. Windows 3.1	P	
b. Windows 95	P	P
c. Windows 98	P	P
d. Windows 2000	P	P
e. Windows NT	P	P
f. MacOS	P	
g. Other		
3. Filters block access to the following (check all appropriate):		
a. Sexually explicit material	P	P
b. Graphic violence	P	P
c. Hate groups	P	P
d. Illegal activity	P	P
e. On-line gambling		P
f. Personals		
g. Occult	P	
h. Web based e-mail		
I. Free ISPs		
j. Other	P	
4. For the categories selected in number 3, do your filters (check all appropriate)		
a. Filter outgoing messages and search requests	P	
Filter incoming messages and search results		
5. How many levels of filtered access do you offer?		
a. 1	P	
b. 2		
c. 3		P
d. 4		
e. 5		
f. More than 5		

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling, and Rating Technologies

	Safexplorer	Stanford University	WinGuardian
2 Product or service works with the following operating systems (Check all appropriate)			
a Windows 3.1			
b Windows 95	P		P
c Windows 98	P		P
d Windows 2000	P		
e Windows NT	P		P
f MacOS			
g Other			
3 Filters block access to the following (check all appropriate):			
a. Sexually explicit material	P	P	
b. Graphic violence	P		
c. Hate groups	P		
d. Illegal activity	P		
e. On-line gambling	P		
f. Personals	P		
g. Occult	P		
h. Web based e-mail	P		
I. Free ISPs	P		
j. Other	P		P
4 For the categories selected in number 3, do your filters (check all appropriate)			
a Filter outgoing messages and search requests	P		P
Filter incoming messages and search results	P	P	
5 How many levels of filtered access do you offer?			
a 1	P	P	
b 2		P	
c 3		P	
d 4		P	
e 5		P	
f More than 5			

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering Labeling and Rating Technologies

	XSTOP.com R2000	Yahoo!
2. Product or service works with the following operating systems (Check all appropriate)		
a. Windows 3.1		P
b. Windows 95	P	P
c. Windows 98	P	P
d. Windows 2000	P	P
e. Windows NT	P	P
f. MacOS		P
g. Other		
3. Filters block access to the following (check all appropriate):		Yahooligans! Is a directory of websites for children ages 7-12. Because the sites are selected individually by editors, all searches are by default "filtered". This is NOT a technology; but rather a result of the human editorial process.
a. Sexually explicit material	P	
b. Graphic violence	P	
c. Hate groups	P	
d. Illegal activity	P	
e. On-line gambling	P	
f. Personals	P	
g. Occult	P	
h. Web based e-mail	P	
I. Free ISPs		
j. Other		None of the above are currently accessible from Yahooligans directory.
4. For the categories selected in number 3, do your filters (check all appropriate)		Yahooligans! Searches are by default "filtered" as a result of how the directory is created and maintained
a. Filter outgoing messages and search requests	P	
Filter incoming messages and search results		
5. How many levels of filtered access do you offer?		
a. 1		P
b. 2		
c. 3		
d. 4		
e. 5		
f. More than 5	P	

812

813

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by *Vendors/Operators of Current Filtering,* Labeling and Rating Technologies

	Zeek Safe (Zeeks.com, Inc.)
2 Product or service works with the following operating systems (Check all appropriate)	
a Windows 3.1	
b Windows 95	P
c Windows 98	P
d Windows 2000	P
e Windows NT	P
f MacOS	
g Other	
3 Filters block access to the following (check all appropriate)	
a. Sexually explicit material	P
b. Graphic violence	P
c. Hate groups	P
d. Illegal activity	P
e. On-line gambling	P
f. Personals	P
g. Occult	P
h. Web based e-mail	
I. Free ISPs	
j. Other	
4 For the categories selected in number 3, do your filters (check all appropriate)	N/A
a Filter outgoing messages and search requests	
Filter incoming messages and search results	
5 How many levels of filtered access do you offer?	
a. 1	P
b. 2	
c. 3	
d. 4	
e. 5	
f. More than 5	

814

815

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling, and Rating Technologies

	Anti-Defamation League Hatefilter (ADL)	Awesome Library Website (EDI)
6. Is the following information available for review (check all appropriate)?		
a. Key word list		
b. Blocked URL list		
c. Criteria for classifying URLs	P	P
Description of filtered categories per access level		
7. Can the subscriber using your product choose to (check all appropriate):		
a. Prevent e-mail coming from/going to specific addresses		
b. Filter e-mail		
c. Allow or disallow attachments		
d. Block spam		
e. Control access to chat		
f. Filter chat		
g. Control access to instant messaging		
h. Filter instant messages		
I. Control access to newsgroups		
j. Filter newsgroup content		
8. Which of the following does this product use to filter content? Check all those that apply.		
a. PICS - compatible ratings		
b. URL lists	P	
c. Human Review		P
d. Key words		
e. Dynamic (real time) review		
Image recognition		
9. If your product filters via image recognition does the image recognition technology filter (check all appropriate):		
a. Web searches		
b. Newsgroups		

316

817

	BASCOM Global Internet	Chaperon 2000
6 Is the following information available for review (check all appropriate)?		
a. Key word list		
b. Blocked URL list	P	
c. Criteria for classifying URLs	P	
Description of filtered categories per access level		
7 Can the subscriber using your product choose to (check all appropriate).		
a. Prevent e-mail coming from/going to specific addresses	P	
b. Filter e-mail	P	
c. Allow or disallow attachments		
d. Block spam		
e. Control access to chat	P	
f. Filter chat		
g. Control access to instant messaging	P	
h. Filter instant messages		
i. Control access to newsgroups	P	
j. Filter newsgroup content		
8 Which of the following does this product use to filter content? Check all those that apply		
a. PICS - compatible ratings		
b. URL lists	P	
c. Human Review	P	
d. Key words		
e. Dynamic (real time) review		Review not real time
Image recognition		
9 If your product filters via image recognition does the image recognition technology filter (check all appropriate):		
a. Web searches	P	
b. Newsgroups	P	

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling, and Rating Technologies

	Characterlink	Childwatch by PACEL Corporation
6. Is the following information available for review (check all appropriate)?		
a. Key word list		
b. Blocked URL list		
c. Criteria for classifying URLs	P	P
Description of filtered categories per access level		
7. Can the subscriber using your product choose to (check all appropriate):		
a. Prevent e-mail coming from/going to specific addresses		
b. Filter e-mail		
c. Allow or disallow attachments		
d. Block spam		
e. Control access to chat		P
f. Filter chat	P	
g. Control access to instant messaging	P	P
h. Filter instant messages	P	
i. Control access to newsgroups	P	
j. Filter newsgroup content	P	
8. Which of the following does this product use to filter content? Check all those that apply		
a. PICS - compatible ratings		
b. URL lists	P	P
c. Human Review	P	
d. Key words		
e. Dynamic (real time) review		
Image recognition		
9. If your product filters via image recognition does the image recognition technology filter (check all appropriate):		
a. Web searches		
b. Newsgroups		

820

821

	Cyber Patrol	Cyber Sentinel V2.0
6. Is the following information available for review (check all appropriate)?		
a. Key word list	P	
b. Blocked URL list		
c. Criteria for classifying URLs	P	
Description of filtered categories per access level	P	
7. Can the subscriber using your product choose to (check all appropriate):		
a. Prevent e-mail coming from/going to specific addresses		P
b. Filter e-mail		P
c. Allow or disallow attachments		
d. Block spam		
e. Control access to chat		P
f. Filter chat	P	P
g. Control access to instant messaging		P
h. Filter instant messages		P
i. Control access to newsgroups	P	P
j. Filter newsgroup content		P
8. Which of the following does this product use to filter content? Check all those that apply.		
a. PICS - compatible ratings	P	
b. URL lists	P	
c. Human Review	P	
d. Key words	optional	P
e. Dynamic (real time) review		P
Image recognition		
9. If your product filters via image recognition does the image recognition technology filter (check all appropriate):		
a. Web searches		
b. Newsgroups		

	CYBERsitter 2000	Desktop Surveillance
6. Is the following information available for review (check all appropriate)?		
a. Key word list		P And User Definable
b. Blocked URL list		
c. Criteria for classifying URLs	P	
Description of filtered categories per access level	P	
7. Can the subscriber using your product choose to (check all appropriate):		
a. Prevent e-mail coming from/going to specific addresses		P
b. Filter e-mail	P	P
c. Allow or disallow attachments		P
d. Block spam		P
e. Control access to chat	P	P
f. Filter chat	P	P
g. Control access to instant messaging	P	P
h. Filter instant messages	P	P
I. Control access to newsgroups	P	P
j. Filter newsgroup content	P	P
8. Which of the following does this product use to filter content? Check all those that apply.		
a. PICS - compatible ratings	P	
b. URL lists	P	
c. Human Review	P	
d. Key words	P	P
e. Dynamic (real time) review	P	
Image recognition		
9. If your product filters via image recognition does the image recognition technology filter (check all appropriate):		
a. Web searches		
b. Newsgroups		

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling and Rating Technologies

	Digimarc Corporation	**Dotsafe, Inc.**
6. Is the following information available for review (check all appropriate)?	This is not directly applicable since the Digimarc watermarking solution is based on the image files themselves not lists, categories or URLs. Our reading technology can be integrated to filter out all images that contain a watermark with an Adult Flag and is included in all images that are not appropriate for minors no matter where they appear.	
a. Key word list		
b. Blocked URL list		
c. Criteria for classifying URLs		
Description of filtered categories per access level	P	P
7. Can the subscriber using your product choose to (check all appropriate)		
a. Prevent e-mail coming from/going to specific addresses		Filtered email acct incl
b. Filter e-mail		P
c. Allow or disallow attachments		P
d. Block spam		
e. Control access to chat	P	
f. Filter chat	P	
g. Control access to instant messaging		
h. Filter instant messages		
I. Control access to newsgroups		P
j. Filter newsgroup content		
8. Which of the following does this product use to filter content? Check all those that apply.		
a. PICS - compatible ratings		P
b. URL lists		P
c. Human Review		P
d. Key words		
e. Dynamic (real time) review		
Image recognition		
9. If your product filters via image recognition does the image recognition technology filter (check all appropriate):		
a. Web searches	P	
b. Newsgroups	P	

826

827

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling and Rating Technologies

	E-Junk, Obvious Solutions	FamilyClick.com, LLC	FamilyConnect
6. Is the following information available for review (check all appropriate)?			
a. Key word list	P		P
b. Blocked URL list			P
c. Criteria for classifying URLs		P	P
Description of filtered categories per access level	P	P	
7. Can the subscriber using your product choose to (check all appropriate):			
a. Prevent e-mail coming from/going to specific addresses	P	P	
b. Filter e-mail	P	P	
c. Allow or disallow attachments	P	P	
d. Block spam	P	P	
e. Control access to chat		P	
f. Filter chat		P	
g. Control access to instant messaging		P	
h. Filter instant messages			
I. Control access to newsgroups		P	P
j. Filter newsgroup content		P	
8. Which of the following does this product use to filter content? Check all those that apply			
a. PICS - compatible ratings		P	
b. URL lists		P	P
c. Human Review		P	P
d. Key words	P	P	P
e. Dynamic (real time) review		P	
Image recognition			
9. If your product filters via image recognition does the image recognition technology filter (check all appropriate):			
a. Web searches			
b. Newsgroups			

829

829

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling, and Rating Technologies

	iForAll	Integrity Online	Integrity Online
6. Is the following information available for review (check all appropriate)?			
a. Key word list	P		
b. Blocked URL list	P		
c. Criteria for classifying URLs	P	P	
Description of filtered categories per access level		P	
7. Can the subscriber using your product choose to (check all appropriate):			
a. Prevent e-mail coming from/going to specific addresses		P	P
b. Filter e-mail	P		P
c. Allow or disallow attachments			
d. Block spam	P		
e. Control access to chat	P	P	
f. Filter chat	P	P	
g. Control access to instant messaging			
h. Filter instant messages			
i. Control access to newsgroups			
j. Filter newsgroup content		P	
8. Which of the following does this product use to filter content? Check all those that apply			
a. PICS - compatible ratings	P		P
b. URL lists	P	P	P
c. Human Review	P	P	P
d. Key words	P		P
e. Dynamic (real time) review	P		P
Image recognition			P
9. If your product filters via image recognition does the image recognition technology filter (check all appropriate):			
a. Web searches			P
b. Newsgroups			P

830

831

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling and Rating Technologies

	Internet Safari, by	**ITECH INC.**
6 Is the following information available for review (check all appropriate)?	Available to select individuals/groups/company under executed non-disclosure agreement.	
a Key word list	P	Locally determined.
b Blocked URL list	P	Public query for URL, filter type and age level.
c Criteria for classifying URLs	P	P
Description of filtered categories per access level	P	Locally determined.
7 Can the subscriber using your product choose to (check all appropriate):		The iTech email filter is a separate product. It includes a web reader, a mail server and a mail spam/filter component
a Prevent e-mail coming from/going to specific addresses		P
b Filter e-mail	P	P
c Allow or disallow attachments		P
d Block spam	via html email program against known spam url and word list	P
e Control access to chat	Chat is not supported.	P
f Filter chat	through http	P
g Control access to instant messaging	instant messaging is not supported	
h Filter instant messages		
i Control access to newsgroups		P
j Filter newsgroup content		
8 Which of the following does this product use to filter content? Check all those that apply		To generate the list, we use human review. In that same sense we also use artificial intelligence, statistical analysis and a wide variety of Internet characteristics and services to generate candidates. However, the decision about including an item in a blocking list is
a PICS - compatible ratings		P
b URL lists	P	P
c Human Review	P	P
d Key words	P	P
e Dynamic (real time) review	P	P
Image recognition	Through a proprietary, patent-pending routine developed by Heartsoft and integrated into Internet Safari	
9 If your product filters via image recognition does the image recognition technology filter (check all appropriate):		
a Web searches	P	
b Newsgroups	newsgroups are not supported in this browser	

	Microsoft IE5 Content Advisor
6. Is the following information available for review (check all appropriate)?	
a. Key word list	
b. Blocked URL list	
c. Criteria for classifying URLs	
Description of filtered categories per access level	P
7. Can the subscriber using your product choose to (check all appropriate):	
a. Prevent e-mail coming from/going to specific addresses	
b. Filter e-mail	
c. Allow or disallow attachments	
d. Block spam	
e. Control access to chat	
f. Filter chat	
g. Control access to instant messaging	
h. Filter instant messages	
i. Control access to newsgroups	
j. Filter newsgroup content	
8. Which of the following does this product use to filter content? Check all those that apply	
a. PICS - compatible ratings	P
b. URL lists	
c. Human Review	
d. Key words	
e. Dynamic (real time) review	
Image recognition	
9. **If your product filters via image recognition does the image recognition technology filter (check all appropriate):**	
a. **Web searches**	
b. **Newsgroups**	

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling, and Rating Technologies

	N2H2
6 Is the following information available for review (check all appropriate)?	
a. Key word list	
b. Blocked URL list	
c. Criteria for classifying URLs	P
Description of filtered categories per access level	P
7 Can the subscriber using your product choose to (check all appropriate):	
a. Prevent e-mail coming from/going to specific addresses	(Web based free e-mail can be blocked)
b. Filter e-mail	N2H2's filtering appliances are usually configured to block access to web-based "free e-mail" services. In addition, a firewall or router configured to only allow e-mail by authorized users who have e-mail accounts on the specific e-mail serve that users have access to. IRC chat, Instant Messages and Newsgroup access
c. Allow or disallow attachments	
d. Block spam	
e. Control access to chat	P (web based chat)
f. Filter chat	P
g. Control access to instant messaging	N2H2's filtering appliances are usually configured to block access to web-based "free e-mail" services. In addition, a firewall or router configured to only allow e-mail by authorized users who have e-mail accounts on the specific e-mail serve that users have access to. IRC chat, Instant Messages and Newsgroup access
h. Filter instant messages	
I. Control access to newsgroups	
j. Filter newsgroup content	P (web based access to newsgroups)
8 Which of the following does this product use to filter content? Check all those that apply.	
a. PICS - compatible ratings	
b. URL lists	P
c. Human Review	P
d. Key words	P
e. Dynamic (real time) review	
Image recognition	
9 If your product filters via image recognition does the image recognition technology filter (check all appropriate):	
a. Web searches	
b. Newsgroups	

836

837

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling, and Rating Technologies

	Net Nanny Software, Inc.	PlanetGood Technologies, Inc.
6. Is the following information available for review (check all appropriate)?		
a. Key word list	P	
b. Blocked URL list	P	
c. Criteria for classifying URLs	Yes-"content generally considered to be inappropriate for	P
Description of filtered categories per access level		
7. Can the subscriber using your product choose to (check all appropriate):		
a. Prevent e-mail coming from/going to specific addresses	Yes - unencrypted e-mail	
b. Filter e-mail	P unencrypted e-mail	
c. Allow or disallow attachments		
d. Block spam		
e. Control access to chat		P
f. Filter chat	,P	
g. Control access to instant messaging		P
h. Filter instant messages	P	
i. Control access to newsgroups	P	P
j. Filter newsgroup content	P	
8. Which of the following does this product use to filter content? Check all those that apply		
a. PICS - compatible ratings		P
b. URL lists	P	P
c. Human Review	P	P
d. Key words	P	P
e. Dynamic (real time) review		
Image recognition		
9. If your product filters via image recognition does the image recognition technology filter (check all appropriate):	N/A	
a. Web searches		
b. Newsgroups		

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering Labeling and Rating Technologies

	REALTIME SENTRY	RSACi, Internet Content Rating Services/
6 Is the following information available for review (check all appropriate)?		
a. Key word list		
b. Blocked URL list		
c. Criteria for classifying URLs		
Description of filtered categories per access level		P
7 Can the subscriber using your product choose to (check all appropriate):	Allows use of current e-mail system	
a. Prevent e-mail coming from/going to specific addresses		
b. Filter e-mail		
c. Allow or disallow attachments		
d. Block spam		
e. Control access to chat		
f. Filter chat		
g. Control access to instant messaging		
h. Filter instant messages		
I. Control access to newsgroups		
j. Filter newsgroup content		
8 Which of the following does this product use to filter content? Check all those that apply		
a. PICS - compatible ratings		P
b. URL lists		
c. Human Review		
d. Key words		
e. Dynamic (real time) review	P	
Image recognition		
9 If your product filters via image recognition does the image recognition technology filter (check all appropriate):		
a. Web searches	P	
b. Newsgroups		

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling and Rating Technologies

	Safe Access	SafeSurf Internet Filtering Solution
6. Is the following information available for review (check all appropriate)?		
a. Key word list		
b. Blocked URL list		
c. Criteria for classifying URLs		P
Description of filtered categories per access level	P	
7. Can the subscriber using your product choose to (check all appropriate):		
a. Prevent e-mail coming from/going to specific addresses		
b. Filter e-mail		
c. Allow or disallow attachments		
d. Block spam		
e. Control access to chat		
f. Filter chat		
g. Control access to instant messaging		
h. Filter instant messages		
i. Control access to newsgroups		
j. Filter newsgroup content		
8. Which of the following does this product use to filter content? Check all those that apply.		
a. PICS - compatible ratings	P	P
b. URL lists	P	P
c. Human Review	P	P
d. Key words		P
e. Dynamic (real time) review		P
Image recognition		
9. If your product filters via image recognition does the image recognition technology filter (check all appropriate):		
a. Web searches		P
b. Newsgroups		

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling and Rating Technologies

	Safexplorer	Stanford University	WinGuardian
6. Is the following information available for review (check all appropriate)?			
a. Key word list	P		
b. Blocked URL list	P		
c. Criteria for classifying URLs			
Description of filtered categories per access level	P		
7. Can the subscriber using your product choose to (check all appropriate):			
a. Prevent e-mail coming from/going to specific addresses	P		
b. Filter e-mail		P	
c. Allow or disallow attachments	P	P	
d. Block spam	P		
e. Control access to chat	P		
f. Filter chat		P	
g. Control access to instant messaging	P		
h. Filter instant messages		P	
I. Control access to newsgroups	P		
j. Filter newsgroup content			
8. Which of the following does this product use to filter content? Check all those that apply			
a. PICS - compatible ratings			
b. URL lists	P		
c. Human Review	P		
d. Key words	P		
e. Dynamic (real time) review	P		
Image recognition		P	P
9. If your product filters via image recognition does the image recognition technology filter (check all appropriate):			
a. Web searches		In demonstrations	P
b. Newsgroups		Possible	P

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling, and Rating Technologies

	XSTOP.com R2000	Yahoo!
6. Is the following information available for review (check all appropriate)?		
a. Key word list	P	
b. Blocked URL list	P	
c. Criteria for classifying URLs	P	http://help.yahoo.com/help/us/yahooligans/
Description of filtered categories per access level	P	
7. Can the subscriber using your product choose to (check all appropriate):		
a. Prevent e-mail coming from/going to specific addresses		P
b. Filter e-mail	P	
c. Allow or disallow attachments		
d. Block spam	P	Spam is filtered into its own folder
e. Control access to chat		
f. Filter chat		Users can filter for language: weak & strong language
g. Control access to instant messaging		
h. Filter instant messages		P
i. Control access to newsgroups	P	
j. Filter newsgroup content		
8. Which of the following does this product use to filter content? Check all those that apply		
a. PICS - compatible ratings		
b. URL lists	P	
c. Human Review	P	Yahooligans!
d. Key words		Geocities uses key words to prevent searches inappropriate
e. Dynamic (real time) review		
Image recognition		
9. If your product filters via image recognition does the image recognition technology filter (check all appropriate):		N/A
a. Web searches		
b. Newsgroups		

846

847

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling and Rating Technologies

	Zeek Safe (Zeeks.com, Inc.)
6 Is the following information available for review (check all appropriate)?	
a Key word list	
b Blocked URL list	
c Criteria for classifying URLs	
Description of filtered categories per access level	P
7 Can the subscriber using your product choose to (check all appropriate):	N/A
a Prevent e-mail coming from/going to specific addresses	
b Filter e-mail	
c Allow or disallow attachments	
d Block spam	
e Control access to chat	
f Filter chat	
g Control access to instant messaging	
h Filter instant messages	
i Control access to newsgroups	
j Filter newsgroup content	
8 Which of the following does this product use to filter content? Check all those that apply	
a PICS - compatible ratings	P
b URL lists	P
c Human Review	P
d Key words	P
e Dynamic (real time) review	
Image recognition	
9 If your product filters via image recognition does the image recognition technology filter (check all appropriate):	N/A
a Web searches	
b Newsgroups	

	Anti-Defamation League Hatefilter (ADL)	Awesome Library Website (EDI)
c E-mail		
d E-mail attachments		
e Chat Rooms		
f Instant Messages		
10 Filtering options		
a Administrator can choose among content categories	P	
b Administrator can permanently edit list of filtered sites		
c Administrator can override company list		
d Administrator can add to company list		
e Administrator develops his own list		
f Administrator has no control		P

	BASCOM Global Internet	**Chaperon 2000**
c E-mail	P	
d E-mail attachments	P	
e Chat Rooms	P	
f Instant Messages	P	
10 Filtering options		
a Administrator can choose among content categories	P	
b Administrator can permanently edit list of filtered sites	P	
c Administrator can override company list	P	
d Administrator can add to company list	P	
e Administrator develops his own list	P	
f Administrator has no control		

852

	Characterlink	Childwatch by PACEL Corporation
c E-mail		
d E-mail attachments		
e Chat Rooms		
f Instant Messages		
10 Filtering options		
a Administrator can choose among content categories	P	
b Administrator can permanently edit list of filtered sites		P
c Administrator can override company list		P
d Administrator can add to company list	P	P
e Administrator develops his own list	P	P
f Administrator has no control		

	Cyber Patrol	Cyber Sentinel V2.0
c. E-mail		
d. E-mail attachments		
e. Chat Rooms		
f. Instant Messages		
10. Filtering options		
a. Administrator can choose among content categories	P	P
b. Administrator can permanently edit list of filtered sites	P	P
c. Administrator can override company list	P	P
d. Administrator can add to company list	P	P
e. Administrator develops his own list	P	P
f. Administrator has no control		

856

857

	CYBERsitter 2000	**Desktop Surveillance**
c. E-mail		
d. E-mail attachments		
e. Chat Rooms		
f. Instant Messages		
10 Filtering options		
a. Administrator can choose among content categories	P	P
b. Administrator can permanently edit list of filtered sites		P
c. Administrator can override company list	P	P
d. Administrator can add to company list	P	P
e. Administrator develops his own list	P	P
f. Administrator has no control		

	Digimarc Corporation	**Dotsafe, Inc.**
c. E-mail	P	
d. E-mail attachments	P	
e. Chat Rooms	P	
f. Instant Messages	P	
10. Filtering options	Utilizing watermarks to filter adult content is not dependent on lists, however it does let the administrator set preferences according to their needs.	
a. Administrator can choose among content categories	P	P
b. Administrator can permanently edit list of filtered sites		
c. Administrator can override company list		P
d. Administrator can add to company list	P	P
e. Administrator develops his own list		
f. Administrator has no control		

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering Labeling and Rating Technologies

	E-Junk, Obvious Solutions	FamilyClick.com, LLC	FamilyConnect
c E-mail			
d E-mail attachments			
e Chat Rooms			
f Instant Messages			
10 Filtering options			
a Administrator can choose among content categories	P	P	
b Administrator can permanently edit list of filtered sites	P		
c Administrator can override company list			
d Administrator can add to company list	P		
e Administrator develops his own list	P		
f Administrator has no control			P

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling and Rating Technologies

	iForAll	Integrity Online	Integrity Online
c. E-mail			
d. E-mail attachments			
e. Chat Rooms			P
f. Instant Messages			
10. Filtering options			
a. Administrator can choose among content categories			
b. Administrator can permanently edit list of filtered sites	P		
c. Administrator can override company list	P		P
d. Administrator can add to company list	P	P	P
e. Administrator develops his own list	P		P
f. Administrator has no control			

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering Labeling and Rating Technologies

	Internet Safari, by	**ITECH INC.**
c E-mail	P	
d E-mail attachments	P	
e Chat Rooms	Chat is not supported in this browser	
f Instant Messages	Instant messages are not support in this browser	
10 Filtering options		There is an optional "access only" list. There is also an local add to the iTech list. In these cases, the local administrator has the option of "developing" his/her own list. It is an option, not a requirement to use the filter.
a Administrator can choose among content categories	P	P
b Administrator can permanently edit list of filtered sites		P
c Administrator can override company list	P	P
d Administrator can add to company list		P
e Administrator develops his own list		P
f Administrator has no control		

	Microsoft IE5 Content Advisor
c. E-mail	
d. E-mail attachments	
e. Chat Rooms	
f. Instant Messages	
10. Filtering options	
a. Administrator can choose among content categories	P
b. Administrator can permanently edit list of filtered sites	
c. Administrator can override company list	
d. Administrator can add to company list	
e. Administrator develops his own list	
f. Administrator has no control	

	N2H2
c E-mail	
d E-mail attachments	
e Chat Rooms	
f Instant Messages	
10 Filtering options	
a Administrator can choose among content categories	P
b Administrator can permanently edit list of filtered sites	P
c Administrator can override company list	P
d Administrator can add to company list	P
e Administrator develops his own list	P
f Administrator has no control	

	Net Nanny Software, Inc.	**PlanetGood Technologies, Inc.**
c E-mail		
d E-mail attachments		
e Chat Rooms		
f Instant Messages		
10 Filtering options		
a Administrator can choose among content categories		P
b Administrator can permanently edit list of filtered sites	P	
c Administrator can override company list	P	P except pornography
d Administrator can add to company list	P	P by submitting the site
e Administrator develops his own list	P	
f Administrator has no control		

	REALTIME SENTRY	RSACi, Internet Content Rating Services/
c E-mail	P	
d E-mail attachments	P	
e Chat Rooms		
f Instant Messages		
10 Filtering options		
a Administrator can choose among content categories		P
b Administrator can permanently edit list of filtered sites		
c Administrator can override company list		
d Administrator can add to company list		
e Administrator develops his own list		
f Administrator has no control	P	

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling and Rating Technologies

	Safe Access	**SafeSurf Internet Filtering Solution**
c E-mail		
d E-mail attachments		
e Chat Rooms		
f Instant Messages		
10 Filtering options		
a Administrator can choose among content categories	P	P
b Administrator can permanently edit list of filtered sites	P	P
c Administrator can override company list	P	P
d Administrator can add to company list	P	P
e Administrator develops his own list		P
f Administrator has no control		

876

877

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering Labeling and Rating Technologies

	Safexplorer	Stanford University	WinGuardian
c E-mail		Possible	P
d E mail attachments		Possible	P
e Chat Rooms		Possible	P
f Instant Messages		Unlikely	P
10. Filtering options			
a Administrator can choose among content categories		P	
b Administrator can permanently edit list of filtered sites	P	Ibid	
c Administrator can override company list	P	Ibid	
d Administrator can add to company list	P	Ibid	
e Administrator develops his own list	P	Ibid	
f Administrator has no control		Ibid	

	XSTOP.com R2000	**Yahoo!**
c. E-mail		
d. E-mail attachments		
e. Chat Rooms		
f. Instant Messages		
10. Filtering options		N/A
a. Administrator can choose among content categories	P	
b. Administrator can permanently edit list of filtered sites	P	
c. Administrator can override company list	P	
d. Administrator can add to company list	P	
e. Administrator develops his own list	P	
f. Administrator has no control		

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling and Rating Technologies

	Zeek Safe (Zeeks.com, Inc.)
c. E-mail	
d. E-mail attachments	
e. Chat Rooms	
f. Instant Messages	
10. Filtering options	
a. Administrator can choose among content categories	P
b. Administrator can permanently edit list of filtered sites	
c. Administrator can override company list	P
d. Administrator can add to company list	P
e. Administrator develops his own list	
f. Administrator has no control	

882

883

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering Labeling and Rating Technologies

	Anti-Defamation League Hatefilter (ADL)	Awesome Library Website (EDI)
11. Which of the following filtering options apply to your product or service?		
a. Unfiltered access until the client opts for filtered		
b. Filtered access until client opts for filtered		
c. Filtered access without a client opt out option		P
d. Client can enable/disable the filters with a password?	P	
12. How long has your product been commercially available?		
a. Less than 1 year		
b. 1 to 2 years	P	P
c. 2 to 3 years		
d. 3 to 4 years		
e. Greater than 4 years		
13. Which of the following describes the size of your business?		
a. 0 to 25,000 customers	P	P
b. 25,000 to 50,000 customers		
c. 50,000 to 100,000 customers		
d. 100,000 to 500,000 customers		
e. Over 500,000 customers		
14. Which of the following describe your Site review process (check all appropriate)		
a. Customers can submit sites for review they believe should be filtered	P	
b. Customers can submit sites for review they believe should not be filtered	P	P
c. All requests are personally responded to	P	Most are
d. You do not have a formal site review process		
15. Which markets does your product/service serve (check all appropriate)?		
a. Homes		P
b. Schools		P
c. Libraries		P
d. Businesses		P
16. Has your product received any of the following (check all appropriate)?		
a. An independent third party evaluation	P	P
b. An independent third party validation	P	
c. An independent third party endorsement?	P	P

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling and Rating Technologies

	BASCOM Global Internet	Chaperon 2000
11 Which of the following filtering options apply to your product or service?		
a Unfiltered access until the client opts for filtered		
b Filtered access until client opts for filtered		
c Filtered access without a client opt out option		
d Client can enable/disable the filters with a password?	P	
12 How long has your product been commercially available?		
a Less than 1 year		
b 1 to 2 years		
c 2 to 3 years		
d 3 to 4 years		
e Greater than 4 years	P	
13 Which of the following describes the size of your business?		
a 0 to 25,000 customers	P	
b 25,000 to 50,000 customers		
c 50,000 to 100,000 customers		
d 100,000 to 500,000 customers		
e Over 500,000 customers		
14 Which of the following describe your Site review process (check all appropriate)		
a Customers can submit sites for review they believe should be filtered		
b Customers can submit sites for review they believe should not be filtered		
c All requests are personally responded to	P	
d You do not have a formal site review process		
15 Which markets does your product/service serve (check all appropriate)?		
a Homes		P (in the future)
b Schools	P	
c Libraries	P	
d Businesses	P	
16 Has your product received any of the following (check all appropriate)?	None	
a An independent third party evaluation		
b An independent third party validation		
c An independent third party endorsement?		

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling and Rating Technologies

	Characterlink	Childwatch by PACEL Corporation
11 Which of the following filtering options apply to your product or service?		
a. Unfiltered access until the client opts for filtered		P
b. Filtered access until client opts for filtered		
c. Filtered access without a client opt out option	P	
d. Client can enable/disable the filters with a password?		P
12. How long has your product been commercially available?		
a. Less than 1 year		P
b. 1 to 2 years		
c. 2 to 3 years		
d. 3 to 4 years	P	
e. Greater than 4 years		
13. Which of the following describes the size of your business?		
a. 0 to 25,000 customers	P	P
b. 25,000 to 50,000 customers		
c. 50,000 to 100,000 customers		
d. 100,000 to 500,000 customers		
e. Over 500,000 customers		
14. Which of the following describe your Site review process (check all appropriate)		
a. Customers can submit sites for review they believe should be filtered	P	P
b. Customers can submit sites for review they believe should not be filtered	P	
c. All requests are personally responded to	P	P
d. You do not have a formal site review process		
15. Which markets does your product/service serve (check all appropriate)?		
a. Homes	P	P
b. Schools	P	
c. Libraries	P	
d. Businesses	P	
16. Has your product received any of the following (check all appropriate)?		
a. An independent third party evaluation		
b. An independent third party validation		
c. An independent third party endorsement?		

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling, and Rating Technologies

	Cyber Patrol	Cyber Sentinel V2.0
11. Which of the following filtering options apply to your product or service?		
a. Unfiltered access until the client opts for filtered	P	
b. Filtered access until client opts for filtered		
c. Filtered access without a client opt out option		
d. Client can enable/disable the filters with a password?	P	P
12. How long has your product been commercially available?		
a. Less than 1 year		
b. 1 to 2 years		
c. 2 to 3 years		P
d. 3 to 4 years		
e. Greater than 4 years	P	
13. Which of the following describes the size of your business?		
a. 0 to 25,000 customers		
b. 25,000 to 50,000 customers		
c. 50,000 to 100,000 customers		
d. 100,000 to 500,000 customers		
e. Over 500,000 customers	P	P
14. Which of the following describe your Site review process (check all appropriate)		
a. Customers can submit sites for review they believe should be filtered	P	P
b. Customers can submit sites for review they believe should not be filtered	P	P
c. All requests are personally responded to	P	P
d. You do not have a formal site review process		
15. Which markets does your product/service serve (check all appropriate)?		
a. Homes	P	P
b. Schools	P	P
c. Libraries	P	P
d. Businesses	P	P
16. Has your product received any of the following (check all appropriate)?		
a. An independent third party evaluation	P	
b. An independent third party validation	P	
c. An independent third party endorsement?	P	

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling and Rating Technologies

	CYBERsitter 2000	Desktop Surveillance
11 Which of the following filtering options apply to your product or service?		
a Unfiltered access until the client opts for filtered		P
b Filtered access until client opts for filtered		
c Filtered access without a client opt out option		P
d Client can enable/disable the filters with a password?	P	P
12 How long has your product been commercially available?		
a Less than 1 year		
b 1 to 2 years		
c 2 to 3 years		P
d 3 to 4 years		
e Greater than 4 years	P	
13. Which of the following describes the size of your business?		
a 0 to 25,000 customers		P
b. 25,000 to 50,000 customers		
c 50,000 to 100,000 customers		
d. 100,000 to 500,000 customers		
e. Over 500,000 customers	P	
14 Which of the following describe your Site review process (check all appropriate)		N/A
a Customers can submit sites for review they believe should be filtered	P	
b Customers can submit sites for review they believe should not be filtered		
c All requests are personally responded to		
d You do not have a formal site review process		
15 Which markets does your product/service serve (check all appropriate)?		
a Homes	P	P
b Schools	P	P
c Libraries	P	P
d Businesses	P	P
16 Has your product received any of the following (check all appropriate)?		
a An independent third party evaluation	P	P
b An independent third party validation		P
c An independent third party endorsement?	P	P

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling, and Rating Technologies

	Digimarc Corporation	Dotsafe, Inc.
11. Which of the following filtering options apply to your product or service?		
a. Unfiltered access until the client opts for filtered	P	
b. Filtered access until client opts for filtered		
c. Filtered access without a client opt out option		
d. Client can enable/disable the filters with a password?		P
12. How long has your product been commercially available?		
a. Less than 1 year		
b. 1 to 2 years		P
c. 2 to 3 years		
d. 3 to 4 years		
e. Greater than 4 years	P	
13. Which of the following describes the size of your business?		
a. 0 to 25,000 customers		
b. 25,000 to 50,000 customers		
c. 50,000 to 100,000 customers		
d. 100,000 to 500,000 customers	P	
e. Over 500,000 customers		P
14. Which of the following describe your Site review process (check all appropriate)	This is not needed with the Digimarc watermark filtering solution	
a. Customers can submit sites for review they believe should be filtered		P
b. Customers can submit sites for review they believe should not be filtered		P
c. All requests are personally responded to		P
d. You do not have a formal site review process		P
15. Which markets does your product/service serve (check all appropriate)?		
a. Homes	P	P
b. Schools	P	P
c. Libraries	P	
d. Businesses	P	P
16. Has your product received any of the following (check all appropriate)?		
a. An independent third party evaluation	P	P
b. An independent third party validation	P	P
c. An independent third party endorsement?	P	P

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling, and Rating Technologies

	E-Junk, Obvious Solutions	FamilyClick.com, LLC	FamilyConnect
11. Which of the following filtering options apply to your product or service?			
a. Unfiltered access until the client opts for filtered			
b. Filtered access until client opts for filtered			
c. Filtered access without a client opt out option	P	P	P
d. Client can enable/disable the filters with a password?			
12. How long has your product been commercially available?			
a. Less than 1 year		P	
b. 1 to 2 years			
c. 2 to 3 years	P		
d. 3 to 4 years			P
e. Greater than 4 years			
13. Which of the following describes the size of your business?			
a. 0 to 25,000 customers	P	P	P
b. 25,000 to 50,000 customers			
c. 50,000 to 100,000 customers			
d. 100,000 to 500,000 customers			
e. Over 500,000 customers			
14. Which of the following describe your Site review process (check all appropriate)			
a. Customers can submit sites for review they believe should be filtered		P	P
b. Customers can submit sites for review they believe should not be filtered		P	P
c. All requests are personally responded to		P	
d. You do not have a formal site review process	P		
15. Which markets does your product/service serve (check all appropriate)?			
a. Homes		P	P
b. Schools	P	P	P
c. Libraries	P		P
d. Businesses	P		P
16. Has your product received any of the following (check all appropriate)?			
a. An independent third party evaluation		P	P
b. An independent third party validation			
c. An independent third party endorsement?		P	P

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling and Rating Technologies

	iForAll	Integrity Online	Integrity Online
11. Which of the following filtering options apply to your product or service?			
a. Unfiltered access until the client opts for filtered	P		
b. Filtered access until client opts for filtered			
c. Filtered access without a client opt out option		P	
d. Client can enable/disable the filters with a password?	P		P
12. How long has your product been commercially available?			
a. Less than 1 year	P		
b. 1 to 2 years			
c. 2 to 3 years			
d. 3 to 4 years			
e. Greater than 4 years		P	P
13. Which of the following describes the size of your business?			
a. 0 to 25,000 customers	P	www.10627.com	P
b. 25,000 to 50,000 customers			
c. 50,000 to 100,000 customers		www Integrity com	
d. 100,000 to 500,000 customers			
e. Over 500,000 customers			
14. Which of the following describe your Site review process (check all appropriate)			
a. Customers can submit sites for review they believe should be filtered		P	P
b. Customers can submit sites for review they believe should not be filtered		P	P
c. All requests are personally responded to		P	P
d. You do not have a formal site review process	P		
15. Which markets does your product/service serve (check all appropriate)?			
a. Homes	P	P	
b. Schools	P	P	
c. Libraries	P	P	
d. Businesses	P	P	
16. Has your product received any of the following (check all appropriate)?			
a. An independent third party evaluation	P		P
b. An independent third party validation	P	P	
c. An independent third party endorsement?	P	P	P

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling, and Rating Technologies

	Internet Safari, by	ITECH INC.
11 Which of the following filtering options apply to your product or service?		The administrator controls the options. Specific users or specific workstations in the network can be set up to deny client opt out. The password override the filter is optionally available and under local control. Where logins are used along with levels of filter access, a user can choose a more restricted filter level.
a. Unfiltered access until the client opts for filtered		P
b. Filtered access until client opts for filtered	Filtered access until client opts for	P
c. Filtered access without a client opt out option		P
d. Client can enable/disable the filters with a password?	Client can enable/disable the filters with a protected file	P
12 How long has your product been commercially available?		
a. Less than 1 year	Still in development	
b. 1 to 2 years		
c. 2 to 3 years		
d. 3 to 4 years		P
e. Greater than 4 years		
13. Which of the following describes the size of your business?		We take customers to mean users of the server based filters.
a. 0 to 25,000 customers	P	
b. 25,000 to 50,000 customers		
c. 50,000 to 100,000 customers		
d. 100,000 to 500,000 customers		P
e. Over 500,000 customers		
14. Which of the following describe your Site review process (check all appropriate).		
a. Customers can submit sites for review they believe should be filtered	P	P
b. Customers can submit sites for review they believe should not be filtered	P	P
c. All requests are personally responded to		
d. You do not have a formal site review process	The need for a formal review process is under consideration and a final determination will be made when	
15. Which markets does your product/service serve (check all appropriate)?		
a. Homes	P	P
b. Schools	P	P
c. Libraries	P	P
d. Businesses		P
16. Has your product received any of the following (check all appropriate)?	Still under development	
a. An independent third party evaluation		
b. An independent third party validation		
c. An independent third party endorsement?		

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering Labeling and Rating Technologies

	Microsoft IE5 Content Advisor
11. Which of the following filtering options apply to your product or service?	
a. Unfiltered access until the client opts for filtered	P
b. Filtered access until client opts for filtered	
c. Filtered access without a client opt out option	
d. Client can enable/disable the filters with a password?	P
12. How long has your product been commercially available?	
a. Less than 1 year	
b. 1 to 2 years	
c. 2 to 3 years	
d. 3 to 4 years	P
e. Greater than 4 years	
13. Which of the following describes the size of your business?	
a. 0 to 25,000 customers	
b. 25,000 to 50,000 customers	
c. 50,000 to 100,000 customers	
d. 100,000 to 500,000 customers	
e. Over 500,000 customers	P
14. Which of the following describe your Site review process (check all appropriate)	
a. Customers can submit sites for review they believe should be filtered	
b. Customers can submit sites for review they believe should not be filtered	
c. All requests are personally responded to	P
d. You do not have a formal site review process	
15. Which markets does your product/service serve (check all appropriate)?	
a. Homes	P
b. Schools	P
c. Libraries	P
d. Businesses	P
16. Has your product received any of the following (check all appropriate)?	
a. An independent third party evaluation	P
b. An independent third party validation	
c. An independent third party endorsement?	

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling and Rating Technologies

	N2H2
11. Which of the following filtering options apply to your product or service?	
a. Unfiltered access until the client opts for filtered	P
b. Filtered access until client opts for filtered	P
c. Filtered access without a client opt out option	P
d. Client can enable/disable the filters with a password?	P
12. How long has your product been commercially available?	
a. Less than 1 year	
b. 1 to 2 years	
c. 2 to 3 years	
d. 3 to 4 years	
e. Greater than 4 years	P
13. Which of the following describes the size of your business?	
a. 0 to 25,000 customers	
b. 25,000 to 50,000 customers	
c. 50,000 to 100,000 customers	
d. 100,000 to 500,000 customers	
e. Over 500,000 customers	Customer - end users of the filtering system
14. Which of the following describe your Site review process (check all appropriate)	
a. Customers can submit sites for review they believe should be filtered	P
b. Customers can submit sites for review they believe should not be filtered	P
c. All requests are personally responded to	All are personally written. However, redundant review requests for identical
d. You do not have a formal site review process	
15. Which markets does your product/service serve (check all appropriate)?	
a. Homes	P
b. Schools	P
c. Libraries	P
d. Businesses	P
16. Has your product received any of the following (check all appropriate)?	We have yet to see a comprehensive, scientific comparison test done between filtering products to date by any third party. Our new customers, such as a school district generally has had a poor experience with another product or evaluates N2H2 filtering services against 1-3 other options prior to purchasing service from N2H2.
a. An independent third party evaluation	
b. An independent third party validation	
c. An independent third party endorsement?	

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling, and Rating Technologies

	Net Nanny Software, Inc.	PlanetGood Technologies, Inc.
11. Which of the following filtering options apply to your product or service?		
a. Unfiltered access until the client opts for filtered	P	
b. Filtered access until client opts for filtered	P	PlanetGood assigns default characteristics to age groups which can
c. Filtered access without a client opt out option		
d. Client can enable/disable the filters with a password?	P	
12. How long has your product been commercially available?		
a. Less than 1 year		
b. 1 to 2 years		P
c. 2 to 3 years		
d. 3 to 4 years		
e. Greater than 4 years	P	
13. Which of the following describes the size of your business?		
a. 0 to 25,000 customers		P
b. 25,000 to 50,000 customers		
c. 50,000 to 100,000 customers		
d. 100,000 to 500,000 customers		
e. Over 500,000 customers	P	
14. Which of the following describe your Site review process (check all appropriate)		
a. Customers can submit sites for review they believe should be filtered	P	P
b. Customers can submit sites for review they believe should not be filtered	P	P
c. All requests are personally responded to		P
d. You do not have a formal site review process		
15. Which markets does your product/service serve (check all appropriate)?		
a. Homes	P	P
b. Schools	P	P
c. Libraries	P	P
d. Businesses	P	P
16. Has your product received any of the following (check all appropriate)?		
a. An independent third party evaluation	Yes, see attached documentation	
b. An independent third party validation	Yes, see attached documentation	
c. An independent third party endorsement?	Yes, see attached documentation	P

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering Labeling and Rating Technologies

	REALTIME SENTRY	RSACi, Internet Content Rating Services/
11 Which of the following filtering options apply to your product or service?		
a Unfiltered access until the client opts for filtered		P
b Filtered access until client opts for filtered		
c Filtered access without a client opt out option		
d Client can enable/disable the filters with a password?		P
12 How long has your product been commercially available?		
a Less than 1 year	P	
b 1 to 2 years		
c 2 to 3 years		
d 3 to 4 years		P
e Greater than 4 years		
13 Which of the following describes the size of your business?		
a 0 to 25,000 customers	P	
b 25,000 to 50,000 customers		
c 50,000 to 100,000 customers		
d 100,000 to 500,000 customers		
e Over 500,000 customers		P
14 Which of the following describe your Site review process (check all appropriate)		
a Customers can submit sites for review they believe should be filtered	P	
b Customers can submit sites for review they believe should not be filtered	P	
c All requests are personally responded to	P	P
d You do not have a formal site review process		
15 Which markets does your product/service serve (check all appropriate)?		
a Homes	P	P
b Schools	P	P
c Libraries	P	P
d Businesses	P	P
16 Has your product received any of the following (check all appropriate)?		
a An independent third party evaluation		P
b An independent third party validation		
c An independent third party endorsement?		

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering Labeling and Rating Technologies

	Safe Access	SafeSurf Internet Filtering Solution
11 Which of the following filtering options apply to your product or service?		
a Unfiltered access until the client opts for filtered		
b Filtered access until client opts for filtered		P
c Filtered access without a client opt out option	P	
d Client can enable/disable the filters with a password?		
12 How long has your product been commercially available?		
a Less than 1 year		
b 1 to 2 years		
c 2 to 3 years	P	
d 3 to 4 years		P
e Greater than 4 years		
13 Which of the following describes the size of your business?		
a 0 to 25,000 customers	P	P
b 25,000 to 50,000 customers		
c 50,000 to 100,000 customers		
d 100,000 to 500,000 customers		
e Over 500,000 customers		
14 Which of the following describe your Site review process (check all appropriate)		
a Customers can submit sites for review they believe should be filtered	P	P
b Customers can submit sites for review they believe should not be filtered	P	P
c All requests are personally responded to	P	
d You do not have a formal site review process		P
15 Which markets does your product/service serve (check all appropriate)?		
a Homes	P	P
b Schools	P	P
c Libraries	P	
d Businesses	P	
16 Has your product received any of the following (check all appropriate)?		
a An independent third party evaluation		
b An independent third party validation		
c An independent third party endorsement?		

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling and Rating Technologies

	Safexplorer	Stanford University	WinGuardian
11 Which of the following filtering options apply to your product or service?			
a Unfiltered access until the client opts for filtered		P	
b Filtered access until client opts for filtered	P	Ibid	
c Filtered access without a client opt out option		Ibid	
d Client can enable/disable the filters with a password?	P	Ibid	
12 How long has your product been commercially available?		Not available	
a Less than 1 year	P		
b 1 to 2 years			P
c 2 to 3 years			
d 3 to 4 years			
e Greater than 4 years			
13. Which of the following describes the size of your business?		None	
a 0 to 25,000 customers	P		
b 25,000 to 50,000 customers			
c 50,000 to 100,000 customers			P
d 100,000 to 500,000 customers			
e Over 500,000 customers			
14 Which of the following describe your Site review process (check all appropriate)			
a Customers can submit sites for review they believe should be filtered		Possible	
b Customers can submit sites for review they believe should not be filtered			
c All requests are personally responded to			
d You do not have a formal site review process			
15 Which markets does your product/service serve (check all appropriate)?			
a Homes	P		P
b Schools	P		P
c Libraries	P		P
d Businesses	P		
16 Has your product received any of the following (check all appropriate)?		No, other than paper reviews	
a An independent third party evaluation			
b An independent third party validation			
c An independent third party endorsement?			

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling and Rating Technologies

	XSTOP.com R2000	Yahoo!
11 Which of the following filtering options apply to your product or service?		N/A
a. Unfiltered access until the client opts for filtered		
b. Filtered access until client opts for filtered	P	
c. Filtered access without a client opt out option		
d. Client can enable/disable the filters with a password?	P	
12 How long has your product been commercially available?		
a. Less than 1 year		
b. 1 to 2 years	P	
c. 2 to 3 years		
d. 3 to 4 years		
e. Greater than 4 years		P
13 Which of the following describes the size of your business?		
a. 0 to 25,000 customers		
b. 25,000 to 50,000 customers		
c. 50,000 to 100,000 customers		
d. 100,000 to 500,000 customers	P	
e. Over 500,000 customers		P
14 Which of the following describe your Site review process (check all appropriate):		
a. Customers can submit sites for review they believe should be filtered	P	P
b. Customers can submit sites for review they believe should not be filtered	P	
c. All requests are personally responded to	P	P
d. You do not have a formal site review process		
15 Which markets does your product/service serve (check all appropriate)?		
a. Homes	P	P
b. Schools	P	P
c. Libraries		P
d. Businesses	P	P
16 Has your product received any of the following (check all appropriate)?		
a. An independent third party evaluation	P	
b. An independent third party validation	P	P
c. An independent third party endorsement?		P

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling and Rating Technologies

	Zeek Safe (Zeeks.com, Inc.)
11 Which of the following filtering options apply to your product or service?	
a. Unfiltered access until the client opts for filtered	
b. Filtered access until client opts for filtered	
c. Filtered access without a client opt out option	
d. Client can enable/disable the filters with a password?	P
12 How long has your product been commercially available?	
a. Less than 1 year	
b. 1 to 2 years	P
c. 2 to 3 years	
d. 3 to 4 years	
e. Greater than 4 years	
13 Which of the following describes the size of your business?	
a. 0 to 25,000 customers	
b. 25,000 to 50,000 customers	P
c. 50,000 to 100,000 customers	
d. 100,000 to 500,000 customers	
e. Over 500,000 customers	
14 Which of the following describe your Site review process (check all appropriate)	
a. Customers can submit sites for review they believe should be filtered	P
b. Customers can submit sites for review they believe should not be filtered	P
c. All requests are personally responded to	
d. You do not have a formal site review process	
15 Which markets does your product/service serve (check all appropriate)?	
a. Homes	P
b. Schools	P
c. Libraries	
d. Businesses	
16 Has your product received any of the following (check all appropriate)?	
a. An independent third party evaluation	
b. An independent third party validation	
c. An independent third party endorsement?	GetNetWise

916

917

	Anti-Defamation League Hatefilter (ADL)	Awesome Library Website (EDI)
17 If your product has received a third party evaluation, validation, or endorsement, please identify the organization that provided it and submit documentation showing the third party's evaluation of your product		**See Awesome Library General Question #17 attached. Recognitions and Awards**
		Hundred of respected sites, including state and local libraries, state and local school systems, nonprofit organizations, newspapers, magazines and commercial sites have evaluated and recommended the Awesome Library Website. A sample is enclosed as "Recognitions and Awards". In addition, over 10,000 major sites recommend their viewers to the Awesome Library.
18 Which of the following best describes your company?		
a Single location		P
b Multiple locations, all company owned	P	
c Multiple locations, all franchised		
d Multiple locations, mixture of company and franchise owned		
19 What is the initial cost to use your product? Please indicate whether this is a one time fee, or a monthly charge		
	Free for seven days, $29.95 for three months of free updates, $29.95 for a year of free updates after that.	$395/month for having the database on the client's server, adapted to the client's needs.

	BASCOM Global Internet	**Chaperon 2000**
17 If your product has received a third party evaluation, validation, or endorsement, please identify the organization that provided it and submit documentation showing the third party's evaluation of your product		
18 Which of the following best describes your company?		
a. Single location	P	
b. Multiple locations, all company owned		
c. Multiple locations, all franchised		
d. Multiple locations, mixture of company and franchise owned		
19 What is the initial cost to use your product? Please indicate whether this is a one time fee, or a monthly charge	Price varies according to User	$2,200 for the first year, then a $1,200/year subscription.

	Characterlink	Childwatch by PACEL Corporation
17 If your product has received a third party evaluation, validation, or endorsement, please identify the organization that provided it and submit documentation showing the third party's evaluation of your product.		**See Childwatch General Question #17**
18 Which of the following best describes your company?		
a. Single location		P
b. Multiple locations, all company owned	P	
c. Multiple locations, all franchised		
d. Multiple locations, mixture of company and franchise owned		
19 What is the initial cost to use your product? Please indicate whether this is a one time fee, or a monthly charge.		
	$15 setup fee, then a monthly service fee (after first month)	Free software - $5 to $10 per month for filtering service depending on subscription duration

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling, and Rating Technologies

	Cyber Patrol	Cyber Sentinel V2.0
17. If your product has received a third party evaluation, validation, or endorsement, please identify the organization that provided it and submit documentation showing the third party's evaluation of your product.	**See Cyber Patrol General Questions #17**	
18. Which of the following best describes your company?		
a. Single location	P	
b. Multiple locations, all company owned		P
c. Multiple locations, all franchised		
d. Multiple locations, mixture of company and franchise owned		
19. What is the initial cost to use your product? Please indicate whether this is a one time fee, or a monthly charge	Varies	$34.95 charge, no monthly charge

	CYBERsitter 2000	Desktop Surveillance
17 If your product has received a third party evaluation, validation, or endorsement, please identify the organization that provided it and submit documentation showing the third party's evaluation of your product.	**See Cybersitter General Question #17**	**See Desktop Surveillance General Question #17**
		Ziff Davis Labs - see attached 5 star rating
18 Which of the following best describes your company?		
a. Single location	P	P
b. Multiple locations, all company owned		
c. Multiple locations, all franchised		
d. Multiple locations, mixture of company and franchise owned		
19. What is the initial cost to use your product? Please indicate whether this is a one time fee, or a monthly charge.		
	$39.95 one time charge	$159.00 - one time price

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling, and Rating Technologies

	Digimarc Corporation	**Dotsafe, Inc.**
17. If your product has received a third party evaluation, validation, or endorsement, please identify the organization that provided it and submit documentation showing the third party's evaluation of your product		
	Our products have been reviewed and adopted as the *de facto* standard for watermarking images across the industry, but have not been previously submitted as technology for this filtering purpose	
18. Which of the following best describes your company?		
a. Single location		
b. Multiple locations, all company owned	P	P
c. Multiple locations, all franchised		
d. Multiple locations, mixture of company and franchise owned		
19. What is the initial cost to use your product? Please indicate whether this is a one time fee, or a monthly charge.		Free
	There is no initial or monthly cost associated with the Adult Flag Digimarc watermarking solution. As a public service, Digimarc will waive the SDK (Software Developer's Kit) license fee to allow Internet filtering and browser application vendors to integrate Digimarc watermark reading software to complement their existing filtering solutions. Using Digimarc embedders bundled within millions of copies of Digimarc-enabled imaging and asset management applications already in distribution around the world, content providers can easily watermark their images with the Adult Flag and a unique Digimarc ID that Digimarc will make widely available to content providers to allow them to mark their content as inappropriate for minors.	

	E-Junk, Obvious Solutions	FamilyClick.com, LLC	FamilyConnect
17. If your product has received a third party evaluation, validation, or endorsement, please identify the organization that provided it and submit documentation showing the third party's evaluation of your product		**See FamilyClick General Question #17**	National Coalition for the Protection of Children and Families
18. Which of the following best describes your company?			
a. Single location	P	P	P
b. Multiple locations, all company owned			
c. Multiple locations, all franchised			
d. Multiple locations, mixture of company and franchise owned			
19. What is the initial cost to use your product? Please indicate whether this is a one time fee, or a monthly charge	$2500 Initial Purchase	$21.95 monthly, or $234.95 for the year in advance	Dial-up monthly retail is $19.95, Wholesale available; Filter-only product is free

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling and Rating Technologies

	iForAll	Integrity Online	Integrity Online
17 If your product has received a third party evaluation, validation, or endorsement, please identify the organization that provided it and submit documentation showing the third party's evaluation of your product.			
	CyberAngels		
18 Which of the following best describes your company?			
a. Single location	P		
b. Multiple locations, all company owned			
c. Multiple locations, all franchised		P	P
d. Multiple locations, mixture of company and franchise owned		P	
19 What is the initial cost to use your product? Please indicate whether this is a one time fee, or a monthly charge.			
	$60.00 one time	$22 month dial-up	$21.95 monthly

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling and Rating Technologies

	Internet Safari, by	ITECH INC.
17 If your product has received a third party evaluation, validation, or endorsement, please identify the organization that provided it and submit documentation showing the third party's evaluation of your product		
18 Which of the following best describes your company?		
a Single location	P	P
b Multiple locations, all company owned		
c Multiple locations, all franchised		
d Multiple locations, mixture of company and franchise owned		
19 What is the initial cost to use your product? Please indicate whether this is a one time fee, or a monthly charge		
	$29 95 one time fee	We do not have a standard box or a shrink-wrapped retail product. The question is this form can not be answered.

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling, and Rating Technologies

	Microsoft IE5 Content Advisor
17 If your product has received a third party evaluation, validation, or endorsement, please identify the organization that provided it and submit documentation showing the third party's evaluation of your product.	The Bertelsmann Foundation together with the consultancy firm, Booz Allen, conducted a year long survey of self-regulatory content filtering regimes in the US, Europe and Australia. Over 100 products were reviewed and tested. RSACi was shortlisted and eventually won the Carl Bertelsmann Prize for outstanding innovation and responsibility in the Information Society. Further, both Microsoft Corporation and Netscape evaluated our product and incorprated RSACi as a preloaded filtering system within their respective browsers. We are backed and supported by 18 member companies including: AOL, Bell Canada, British Telecom, Cable & Wireless, Deutsche Telecom, IBM and Microsoft. RSACi was highlighted in both the first and second White House Online Summit and ICRA was recently awarded a $650,000 grant from the European Union after a rigorous evaluation of our mission and product and plans for the future. Finally, over 150,000 sites have rated using the RSACi system including many of the leading sites in the world.
18 Which of the following best describes your company?	
a. Single location	
b. Multiple locations, all company owned	P Not for profit organization
c. Multiple locations, all franchised	
d. Multiple locations, mixture of company and franchise owned	
19 What is the initial cost to use your product? Please indicate whether this is a one time fee, or a monthly charge.	Free

	N2H2
17 If your product has received a third party evaluation, validation, or endorsement, please identify the organization that provided it and submit documentation showing the third party's evaluation of your product.	
	We have yet to see a comprehensive, scientific comparison test done between filtering products to date by any third party. Our new customers, such as a school district generally has had a poor experience with another product or evaluates N2H2 filtering services against 1-3 other options prior to purchasing service from N2H2.
18 Which of the following best describes your company?	
a Single location	
b Multiple locations, all company owned	P
c Multiple locations, all franchised	
d Multiple locations, mixture of company and franchise owned	
19 What is the initial cost to use your product? Please indicate whether this is a one time fee, or a monthly charge.	A one time set up fee is charged to establish N2H2 hardware on a customer's network, then a per user or per workstation fee is charged. Schools have the option of selecting a sponsor supported version of our service that has no recurring fees for the schools. A majority of school districts opt for the sponsored model, those who do not pay approximately $1 per student per year. Corporate Networks pricing varies widely based on the size and capacity of their corporate networks. Home Users have the cost of filtering bundled with their ISP fees. The ISP sets the pricing policies, often the service is free, sometime a fee of $1-3 per month is charged.

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering Labeling and Rating Technologies

	Net Nanny Software, Inc.	PlanetGood Technologies, Inc
17 If your product has received a third party evaluation, validation, or endorsement, please identify the organization that provided it and submit documentation showing the third party's evaluation of your product.	**See Net Nanny General Question #17**	
		Anne Collier, President and director of Net News, said "We think you should know about it because it's a trailblazer." "it's not just a kid browser, not filter or blocking software, not a filtered Internet service provider, not a site rating system - but, in a creative way, PlanetGood combines all those things. And its makers, an Indianapolis-based company called BrowseSafe, very handily hands over to parents all judgment on what is/isn't appropriate Web content for kids.
18 Which of the following best describes your company?		
a. Single location		P
b. Multiple locations, all company owned	P	
c. Multiple locations, all franchised		
d. Multiple locations, mixture of company and franchise owned		
19 What is the initial cost to use your product? Please indicate whether this is a one time fee, or a monthly charge.		
	$34.95 one-time fee	$5 per month

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling, and Rating Technologies

	REALTIME SENTRY	RSACi, Internet Content Rating Services/
17. If your product has received a third party evaluation, validation, or endorsement, please identify the organization that provided it and submit documentation showing the third party's evaluation of your product.		
		The Bertelsmann Foundation together with the consultancy firm, Booz Allen, conducted a year long survey of self-regulatory content filtering regimes in the US, Europe and Australia. Over 100 products were reviewed and tested. RSACi was shortlisted and eventually won the Carol Bertelsmann Prize for outstanding innovation and responsibility in the Information Society. Further, both Microsoft Corporation and Netscape evaluated our product and incorporated RSACi as a preloaded filtering system within their respective browsers. We are backed and supported by 18 member companies including: AOL, Bell Canada, British Telecom, Cable & Wireless, Deutsche Telecom, IBM and Microsoft. RSACi was highlighted in both the first and second White House Online Summit and ICRA was recently awared a $650,000 grant from the European Union after a rigorous evaluation of our mission and product and plans for the future. Finally, oever 150,000 sites have rated using the RSACi system including many of the leading sites in the world.
18. Which of the following best describes your company?		
a. Single location	P	
b. Multiple locations, all company owned		
c. Multiple locations, all franchised		
d. Multiple locations, mixture of company and franchise owned		
19. What is the initial cost to use your product? Please indicate whether this is a one time fee, or a monthly charge.		
	$7.00 per month	

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling, and Rating Technologies

	Safe Access	SafeSurf Internet Filtering Solution
17. If your product has received a third party evaluation, validation, or endorsement, please identify the organization that provided it and submit documentation showing the third party's evaluation of your product		**See Safesurf General Question #17**
18. Which of the following best describes your company?		
a. Single location	P	
b. Multiple locations, all company owned		P
c. Multiple locations, all franchised		
d. Multiple locations, mixture of company and franchise owned		
19. What is the initial cost to use your product? Please indicate whether this is a one time fee, or a monthly charge.	$10 setup fee (one time) $15.95 per month	Fees are negotiated based on requirements of portal/ search engine.

	Safexplorer	Stanford University	WinGuardian
17. If your product has received a third party evaluation, validation, or endorsement, please identify the organization that provided it and submit documentation showing the third party's evaluation of your product.			
18. Which of the following best describes your company?			
a. Single location		P	P
b. Multiple locations, all company owned	P		
c. Multiple locations, all franchised			
d. Multiple locations, mixture of company and franchise owned			
19. What is the initial cost to use your product? Please indicate whether this is a one time fee, or a monthly charge.	$39.95 US for download; $49.95 US for CD and manual (This is a one time fee.)		

	XSTOP.com R2000	Yahoo!
17 If your product has received a third party evaluation, validation, or endorsement, please identify the organization that provided it and submit documentation showing the third party's evaluation of your product	PC Magazine; ICD	Trust e
18 Which of the following best describes your company?		
a. Single location	P	
b. Multiple locations, all company owned		P
c. Multiple locations, all franchised		
d. Multiple locations, mixture of company and franchise owned		
19 What is the initial cost to use your product? Please indicate whether this is a one time fee, or a monthly charge	$12,800 one time; $6,980 Annual Fee	N/A

	Zeek Safe (Zeeks.com, Inc.)
17. If your product has received a third party evaluation, validation, or endorsement, please identify the organization that provided it and submit documentation showing the third party's evaluation of your product.	**See Zeek Safe General Question #17**
18. Which of the following best describes your company?	
a. Single location	P
b. Multiple locations, all company owned	
c. Multiple locations, all franchised	
d. Multiple locations, mixture of company and franchise owned	
19. What is the initial cost to use your product? Please indicate whether this is a one time fee, or a monthly charge.	Free. Monthly updates are also free.

951

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling, and Rating Technologies

	Anti-Defamation League Hatefilter (ADL)	Awesome Library Website (EDI)
B. FOR ISPs WITH FILTERING AVAILABLE		
1. Which server based filtering tool does your service utilize?		
a. N2H2		
b. URLabs I-Gear		
c. Websense		
d. BAIR		
e. Proprietary		
f. Other		
2. In your current capacity, describe your geographic coverage		
a. Local		
b. Regional		
c. National		
d. International		
3. Please check the following features your service provides.		
a. Filtered searches		
b. White list (pre-selected content)		
c. Human Monitored chatrooms		
d. Technology monitored chatrooms		
e. Tamper-proof network		
f. Proprietary Content		
g. Usage monitoring		
h. Web hosting		
4. Are your content policies for Internet content consistent for		
a. Web sites you host		
b. Advertising (banner ads, etc.)		
c. Newsgroup feeds		
5. How do you offer your service?		
a. Dial up (What speeds)		
b. T-1 access		
c. DSL		
d. Broadband		
6. Your service is compatible with a third party's		
a. Dial up (What speeds)		
b. T-1 access		
c. DSL		
d. Broadband		

C. FOR CLIENT SIDE APPLICATIONS		
1. Regarding product updates, does your product		
a. Automatically updates itself?		
b. Customer must download updates	P	
c. Other		Database is updated by Vendor two times per month.
2. Do these updates cost anything?		
a. Free	P	P
b. $1 - $25		
c. $26 - $50		
d. $51 - $100		

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling, and Rating Technologies

	BASCOM Global Internet	Chaperon 2000
B. FOR ISPs WITH FILTERING AVAILABLE		
1. Which server based filtering tool does your service utilize?		
a. N2H2		
b. URLabs I-Gear		
c. Websense		
d. BAIR		
e. Proprietary	P	
f. Other		
2. In your current capacity, describe your geographic coverage		
a. Local	P	
b. Regional		
c. National		
d. International		
3. Please check the following features your service provides.		
a. Filtered searches	P	
b. White list (pre-selected content)	P	
c. Human Monitored chatrooms		
d. Technology monitored chatrooms	P	
e. Tamper-proof network	P	
f. Proprietary Content	P	
g. Usage monitoring	P	
h. Web hosting	P	
4. Are your content policies for Internet content consistent for:		
a. Web sites you host	P	
b. Advertising (banner ads, etc.)	P	
c. Newsgroup feeds	P	
5. How do you offer your service?		
a. Dial up (What speeds)	P	
b. T-1 access	P	
c. DSL	P	
d. Broadband	P	
6. Your service is compatible with a third party's		
a. Dial up (What speeds)	P	
b. T-1 access	P	
c. DSL	P	
d. Broadband	P	

C. FOR CLIENT SIDE APPLICATIONS		
1. Regarding product updates, does your product		
a. Automatically updates itself?	P	
b. Customer must download updates		
c. Other		
2. Do these updates cost anything?		
a. Free	P	
b. $1 - $25		
c. $26 - $50		
d. $51 - $100		

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling and Rating Technologies

	Characterlink	Childwatch by PACEL Corporation
B. FOR ISPs WITH FILTERING AVAILABLE		
1. Which server based filtering tool does your service utilize?		
a. N2H2		
b. URLabs I-Gear		
c. Websense		
d. BAIR		
e. Proprietary	P	
f. Other	P	
2. In your current capacity, describe your geographic coverage		
a. Local		
b. Regional		
c. National		
d. International	P	
3. Please check the following features your service provides		
a. Filtered searches	P	
b. White list (pre-selected content)	P	
c. Human Monitored chatrooms		
d. Technology monitored chatrooms		
e. Tamper-proof network		
f. Proprietary Content		
g. Usage monitoring		
h. Web hosting	P	
4. Are your content policies for Internet content consistent for		
a. Web sites you host	P	
b. Advertising (banner ads, etc.)	P	
c. Newsgroup feeds		
5. How do you offer your service?		
a. Dial up (What speeds)	P v.90 56K	
b. T-1 access		
c. DSL		
d. Broadband		
6. Your service is compatible with a third party's		
a. Dial up (What speeds)	P	
b. T-1 access	P	
c. DSL	P	
d. Broadband	P	

C. FOR CLIENT SIDE APPLICATIONS		
1. Regarding product updates, does your product		
a. Automatically updates itself?		P
b. Customer must download updates		
c. Other		
2. Do these updates cost anything?		
a. Free		P
b. $1 - $25		
c. $26 - $50		
d. $51 - $100		

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling, and Rating Technologies

	Cyber Patrol	Cyber Sentinel V2.0
B. FOR ISPs WITH FILTERING AVAILABLE		
1. Which server based filtering tool does your service utilize?		
a. N2H2		
b. URLabs I-Gear		
c. Websense		
d. BAIR		
e. Proprietary		
f. Other		
2. In your current capacity, describe your geographic coverage		
a. Local		
b. Regional		
c. National		
d. International		
3. Please check the following features your service provides.		
a. Filtered searches		
b. White list (pre-selected content)		
c. Human Monitored chatrooms		
d. Technology monitored chatrooms		
e. Tamper-proof network		
f. Proprietary Content		
g. Usage monitoring		
h. Web hosting		
4. Are your content policies for Internet content consistent for:		
a. Web sites you host		
b. Advertising (banner ads, etc.)		
c. Newsgroup feeds		
5. How do you offer your service?		
a. Dial up (What speeds)		
b. T-1 access		
c. DSL		
d. Broadband		
6. Your service is compatible with a third party's		
a. Dial up (What speeds)		
b. T-1 access		
c. DSL		
d. Broadband		

C. FOR CLIENT SIDE APPLICATIONS		
1. Regarding product updates, does your product		
a. Automatically updates itself?	P	
b. Customer must download updates		
c. Other		P
2. Do these updates cost anything?		
a. Free	P	P
b. $1 - $25		
c. $26 - $50		
d. $51 - $100		

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling, and Rating Technologies

	CYBERsitter 2000	Desktop Surveillance
B. FOR ISPs WITH FILTERING AVAILABLE		
1. Which server based filtering tool does your service utilize?		
a. N2H2		P
b. URLabs I-Gear		P
c. Websense		P
d. BAIR		P
e. Proprietary		P
f. Other		
2. In your current capacity, describe your geographic coverage		
a. Local		
b. Regional		
c. National		
d. International		P
3. Please check the following features your service provides:		
a. Filtered searches		P
b. White list (pre-selected content)		P
c. Human Monitored chatrooms		P
d. Technology monitored chatrooms		P
e. Tamper-proof network		P
f. Proprietary Content		P
g. Usage monitoring		P
h. Web hosting		
4. Are your content policies for Internet content consistent for:		
a. Web sites you host		P
b. Advertising (banner ads, etc.)		P
c. Newsgroup feeds		P
5. How do you offer your service?		
a. Dial up (What speeds)		P
b. T-1 access		P
c. DSL		P
d. Broadband		P
6. Your service is compatible with a third party's		
a. Dial up (What speeds)		P
b. T-1 access		P
c. DSL		P
d. Broadband		P

C. FOR CLIENT SIDE APPLICATIONS		
1. Regarding product updates, does your product		
a. Automatically updates itself?	P	
b. Customer must download updates		P
c. Other	Customers can manually update at will	
2. Do these updates cost anything?		
a. Free	P	P
b. $1 - $25		
c. $26 - $50		
d. $51 - $100		

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling and Rating Technologies

	Digimarc Corporation	Dotsafe, Inc.
B. FOR ISPs WITH FILTERING AVAILABLE		
1. Which server based filtering tool does your service utilize?		
a. N2H2		
b. URLabs I-Gear		
c. Websense		
d. BAIR		
e. Proprietary		P
f. Other		P
2. In your current capacity, describe your geographic coverage		
a. Local		
b. Regional		
c. National		P
d. International		P
3. Please check the following features your service provides:		
a. Filtered searches		
b. White list (pre-selected content)		
c. Human Monitored chatrooms		
d. Technology monitored chatrooms		
e. Tamper-proof network		P
f. Proprietary Content		
g. Usage monitoring		P
h. Web hosting		
4. Are your content policies for Internet content consistent for:		
a. Web sites you host		
b. Advertising (banner ads, etc.)		P
c. Newsgroup feeds		
5. How do you offer your service?		
a. Dial up (What speeds)		P
b. T-1 access		P
c. DSL		P
d. Broadband		P
6. Your service is compatible with a third party's		
a. Dial up (What speeds)		P
b. T-1 access		P
c. DSL		P
d. Broadband		P

C. FOR CLIENT SIDE APPLICATIONS		
1. Regarding product updates, does your product		
a. Automatically updates itself?		
b. Customer must download updates		
c. Other		
2. Do these updates cost anything?		
a. Free		
b. $1 - $25		
c. $26 - $50		
d. $51 - $100		

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling and Rating Technologies

	E-Junk, Obvious Solutions	FamilyClick.com, LLC	FamilyConnect
B. FOR ISPs WITH FILTERING AVAILABLE			
1. Which server based filtering tool does your service utilize?			
a. N2H2			
b. URLabs I-Gear		P	
c. Websense			
d. BAIR			
e. Proprietary		P	P
f. Other		P	
2. In your current capacity, describe your geographic coverage			
a. Local			
b. Regional			
c. National		P	P
d. International			
3. Please check the following features your service provides			
a. Filtered searches		P	P
b. White list (pre-selected content)		P	P
c. Human Monitored chatrooms			
d. Technology monitored chatrooms		P	
e. Tamper-proof network		P	P
f. Proprietary Content		P	
g. Usage monitoring			
h. Web hosting			
4. Are your content policies for Internet content consistent for:			
a. Web sites you host		P	P
b. Advertising (banner ads, etc.)		P	P
c. Newsgroup feeds		P	P
5. How do you offer your service?			
a. Dial up (What speeds)		P	P
b. T-1 access			P
c. DSL			P
d. Broadband			P
6. Your service is compatible with a third party's			
a. Dial up (What speeds)		P	P
b. T-1 access		P	P
c. DSL		P	P
d. Broadband		P	P

C. FOR CLIENT SIDE APPLICATIONS			
1. Regarding product updates, does your product			
a. Automatically updates itself?			
b. Customer must download updates	P		
c. Other			
2. Do these updates cost anything?			
a. Free			
b. $1 - $25			
c. $26 - $50			
d. $51 - $100			

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling, and Rating Technologies

	iForAll	Integrity Online	Integrity Online
B. FOR ISPs WITH FILTERING AVAILABLE			
1. Which server based filtering tool does your service utilize?			
a. N2H2		P	P
b. URLabs I-Gear			
c. Websense			
d. BAIR			
e. Proprietary			
f. Other			
2. In your current capacity, describe your geographic coverage			
a. Local		P Statewide	P
b. Regional			P
c. National			
d. International			
3. Please check the following features your service provides			
a. Filtered searches		P	P
b. White list (pre-selected content)			P
c. Human Monitored chatrooms			P
d. Technology monitored chatrooms			
e. Tamper-proof network		P	
f. Proprietary Content		P	P
g. Usage monitoring		P	
h. Web hosting		P	P
4. Are your content policies for Internet content consistent for			
a. Web sites you host		P	P
b. Advertising (banner ads, etc.)		P	P
c. Newsgroup feeds		P	P
5. How do you offer your service?			
a. Dial up (What speeds)		P 56K	P
b. T-1 access		P	P
c. DSL		P	P
d. Broadband		P	P
6. Your service is compatible with a third party's			
a. Dial up (What speeds)			P
b. T-1 access			P
c. DSL			P
d. Broadband			P

C. FOR CLIENT SIDE APPLICATIONS			
1. Regarding product updates, does your product			
a. Automatically updates itself?			P
b. Customer must download updates	P		
c. Other			
2. Do these updates cost anything?			
a. Free			P
b. $1 - $25			
c. $26 - $50	P		
d. $51 - $100			

966

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling and Rating Technologies

	Internet Safari, by	ITECH INC.
B. FOR ISPs WITH FILTERING AVAILABLE		
1. Which server based filtering tool does your service utilize?		We do not sell an ISP product, iTech's ispFamilyFilter and we would like to see it listed on any future COPA questionnaires--or alternatively--we would ask that not provide a check list of products unless that list is exhaustive.
a. N2H2		
b. URLabs I-Gear		
c. Websense		
d. BAIR		
e. Proprietary		
f. Other		
2. In your current capacity, describe your geographic coverage		
a. Local		
b. Regional		
c. National		
d. International		
3. Please check the following features your service provides		
a. Filtered searches		
b. White list (pre-selected content)		
c. Human Monitored chatrooms		
d. Technology monitored chatrooms		
e. Tamper-proof network		
f. Proprietary Content		
g. Usage monitoring		
h. Web hosting		
4. Are your content policies for Internet content consistent for:		
a. Web sites you host		
b. Advertising (banner ads, etc.)		
c. Newsgroup feeds		
5. How do you offer your service?		
a. Dial up (What speeds)		
b. T-1 access		
c. DSL		
d. Broadband		
6. Your service is compatible with a third party's		
a. Dial up (What speeds)		
b. T-1 access		
c. DSL		
d. Broadband		

C. FOR CLIENT SIDE APPLICATIONS		
1. Regarding product updates, does your product		
a. Automatically updates itself?		
b. Customer must download updates		
c. Other		
2. Do these updates cost anything?		
a. Free		
b. $1 - $25		
c. $26 - $50		
d. $51 - $100		

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling, and Rating Technologies

	Microsoft IE5 Content Advisor
B. FOR ISPs WITH FILTERING AVAILABLE	
1. Which server based filtering tool does your service utilize?	
a. N2H2	
b. URLabs I-Gear	
c. Websense	
d. BAIR	
e. Proprietary	
f. Other	
2. In your current capacity, describe your geographic coverage	
a. Local	
b. Regional	
c. National	
d. International	
3. Please check the following features your service provides:	
a. Filtered searches	
b. White list (pre-selected content)	
c. Human Monitored chatrooms	
d. Technology monitored chatrooms	
e. Tamper-proof network	
f. Proprietary Content	
g. Usage monitoring	
h. Web hosting	
4. Are your content policies for Internet content consistent for:	
a. Web sites you host	
b. Advertising (banner ads, etc.)	
c. Newsgroup feeds	
5. How do you offer your service?	
a. Dial up (What speeds)	
b. T-1 access	
c. DSL	
d. Broadband	
6. Your service is compatible with a third party's	
a. Dial up (What speeds)	
b. T-1 access	
c. DSL	
d. Broadband	

C. FOR CLIENT SIDE APPLICATIONS	
1. Regarding product updates, does your product	
a. Automatically updates itself?	
b. Customer must download updates	
c. Other	
2. Do these updates cost anything?	
a. Free	
b. $1 - $25	
c. $26 - $50	
d. $51 - $100	

970

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling, and Rating Technologies

	N2H2
B. FOR ISPs WITH FILTERING AVAILABLE	
1. Which server based filtering tool does your service utilize?	
a. N2H2	
b. URLabs I-Gear	
c. Websense	
d. BAIR	
e. Proprietary	
f. Other	
2. In your current capacity, describe your geographic coverage	
a. Local	
b. Regional	
c. National	
d. International	
3. Please check the following features your service provides.	
a. Filtered searches	
b. White list (pre-selected content)	
c. Human Monitored chatrooms	
d. Technology monitored chatrooms	
e. Tamper-proof network	
f. Proprietary Content	
g. Usage monitoring	
h. Web hosting	
4. Are your content policies for Internet content consistent for:	
a. Web sites you host	
b. Advertising (banner ads, etc.)	
c. Newsgroup feeds	
5. How do you offer your service?	
a. Dial up (What speeds)	
b. T-1 access	
c. DSL	
d. Broadband	
6. Your service is compatible with a third party's	
a. Dial up (What speeds)	
b. T-1 access	
c. DSL	
d. Broadband	

C. FOR CLIENT SIDE APPLICATIONS	
1. Regarding product updates, does your product	
a. Automatically updates itself?	
b. Customer must download updates	
c. Other	
2. Do these updates cost anything?	
a. Free	
b. $1 - $25	
c. $26 - $50	
d. $51 - $100	

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling, and Rating Technologies

	Net Nanny Software, Inc.	**PlanetGood Technologies, Inc.**
B. FOR ISPs WITH FILTERING AVAILABLE		
1. Which server based filtering tool does your service utilize?		
a. N2H2		
b. URLabs I-Gear		
c. Websense		
d. BAIR		
e. Proprietary		
f. Other		
2. In your current capacity, describe your geographic coverage		
a. Local		
b. Regional		
c. National		
d. International		
3. Please check the following features your service provides:		
a. Filtered searches		
b. White list (pre-selected content)		
c. Human Monitored chatrooms		
d. Technology monitored chatrooms		
e. Tamper-proof network		
f. Proprietary Content		
g. Usage monitoring		
h. Web hosting		
4. Are your content policies for Internet content consistent for:		
a. Web sites you host		
b. Advertising (banner ads, etc.)		
c. Newsgroup feeds		
5. How do you offer your service?		
a. Dial up (What speeds)		
b. T-1 access		
c. DSL		
d. Broadband		
6. Your service is compatible with a third party's		
a. Dial up (What speeds)		
b. T-1 access		
c. DSL		
d. Broadband		

C. FOR CLIENT SIDE APPLICATIONS		
1. Regarding product updates, does your product		
a. Automatically updates itself?		P
b. Customer must download updates		P
c. Other		
2. Do these updates cost anything?		
a. Free		P
b. $1 - $25		
c. $26 - $50		
d. $51 - $100		

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling, and Rating Technologies

	REALTIME SENTRY	RSACi, Internet Content Rating Services/
B. FOR ISPs WITH FILTERING AVAILABLE		
1. Which server based filtering tool does your service utilize?		
a. N2H2		
b. URLabs I-Gear		
c. Websense		
d. BAIR		
e. Proprietary		
f. Other		
2. In your current capacity, describe your geographic coverage		
a. Local		
b. Regional		
c. National		
d. International		
3. Please check the following features your service provides:		
a. Filtered searches		
b. White list (pre-selected content)		
c. Human Monitored chatrooms		
d. Technology monitored chatrooms		
e. Tamper-proof network		
f. Proprietary Content		
g. Usage monitoring		
h. Web hosting		
4. Are your content policies for Internet content consistent for:		
a. Web sites you host		
b. Advertising (banner ads, etc.)		
c. Newsgroup feeds		
5. How do you offer your service?		
a. Dial up (What speeds)		
b. T-1 access		
c. DSL		
d. Broadband		
6. Your service is compatible with a third party's		
a. Dial up (What speeds)		
b. T-1 access		
c. DSL		
d. Broadband		
C. FOR CLIENT SIDE APPLICATIONS		
1. Regarding product updates, does your product		
a. Automatically updates itself?	P	
b. Customer must download updates		
c. Other		
2. Do these updates cost anything?		
a. Free	P	
b. $1 - $25		
c. $26 - $50		
d. $51 - $100		

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling and Rating Technologies

	Safe Access	SafeSurf Internet Filtering Solution
B. FOR ISPs WITH FILTERING AVAILABLE		
1 Which server based filtering tool does your service utilize?		
a N2H2		
b URLabs I-Gear		
c Websense		
d BAIR		
e Proprietary		
f Other	P	
2 In your current capacity, describe your geographic coverage		
a Local		
b Regional		
c National	P	
d International		
3 Please check the following features your service provides		
a Filtered searches	P	
b White list (pre-selected content)		
c Human Monitored chatrooms		
d Technology monitored chatrooms		
e Tamper-proof network	P	
f Proprietary Content		
g Usage monitoring		
h Web hosting	P	
4 Are your content policies for Internet content consistent for		
a Web sites you host	P	
b Advertising (banner ads, etc)	P	
c Newsgroup feeds	P	
5 How do you offer your service?		
a Dial up (What speeds)	P	
b T-1 access	P	
c DSL		
d Broadband	P	
6 Your service is compatible with a third party's		
a Dial up (What speeds)		
b T-1 access		
c DSL		
d Broadband		

C. FOR CLIENT SIDE APPLICATIONS		
1 Regarding product updates, does your product		
a Automatically updates itself?		
b Customer must download updates		
c Other		
2 Do these updates cost anything?		
a Free		
b $1 - $25		
c $26 - $50		
d $51 - $100		

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering Labeling and Rating Technologies

	Safexplorer	Stanford University	WinGuardian
B. FOR ISPs WITH FILTERING AVAILABLE			
1. Which server based filtering tool does your service utilize?			
a. N2H2			
b. URLabs I-Gear			
c. Websense			
d. BAIR			
e. Proprietary			
f. Other			
2. In your current capacity, describe your geographic coverage			
a. Local			
b. Regional			
c. National			
d. International			P
3. Please check the following features your service provides.			
a. Filtered searches			
b. White list (pre-selected content)			
c. Human Monitored chatrooms			
d. Technology monitored chatrooms			P
e. Tamper-proof network			
f. Proprietary Content			
g. Usage monitoring			P
h. Web hosting			
4. Are your content policies for Internet content consistent for			
a. Web sites you host			P
b. Advertising (banner ads, etc.)			P
c. Newsgroup feeds			P
5. How do you offer your service?			
a. Dial up (What speeds)			
b. T-1 access			
c. DSL			
d. Broadband			
6. Your service is compatible with a third party's			
a. Dial up (What speeds)			
b. T-1 access			
c. DSL			
d. Broadband			

C. FOR CLIENT SIDE APPLICATIONS			
1. Regarding product updates, does your product			
a. Automatically updates itself?			
b. Customer must download updates	P		P
c. Other			
2. Do these updates cost anything?			
a. Free	P		
b. $1 - $25			P
c. $26 - $50			
d. $51 - $100			

950

981

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling and Rating Technologies

	XSTOP.com R2000	Yahoo!
B. FOR ISPs WITH FILTERING AVAILABLE		
1. Which server based filtering tool does your service utilize?		
a. N2H2		
b. URLabs I-Gear		
c. Websense		
d. BAIR		
e. Proprietary		
f. Other		
2. In your current capacity, describe your geographic coverage		
a. Local		
b. Regional		
c. National		
d. International		
3. Please check the following features your service provides		
a. Filtered searches		
b. White list (pre-selected content)		
c. Human Monitored chatrooms		
d. Technology monitored chatrooms		
e. Tamper-proof network		
f. Proprietary Content		
g. Usage monitoring		
h. Web hosting		
4. Are your content policies for Internet content consistent for		
a. Web sites you host		
b. Advertising (banner ads, etc.)		
c. Newsgroup feeds		
5. How do you offer your service?		
a. Dial up (What speeds)		
b. T-1 access		
c. DSL		
d. Broadband		
6. Your service is compatible with a third party's		
a. Dial up (What speeds)		
b. T-1 access		
c. DSL		
d. Broadband		

C. FOR CLIENT SIDE APPLICATIONS		
1. Regarding product updates, does your product		
a. Automatically updates itself?	P	
b. Customer must download updates		
c. Other		
2. Do these updates cost anything?		
a. Free		
b. $1 - $25		
c. $26 - $50	P Yearly	
d. $51 - $100		

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering Labeling and Rating Technologies

	Zeek Safe (Zeeks.com, Inc.)
B. FOR ISPs WITH FILTERING AVAILABLE	
1. Which server based filtering tool does your service utilize?	
a. N2H2	P
b. URLabs I-Gear	P
c. Websense	P
d. BAIR	P
e. Proprietary	P
f. Other	
2. In your current capacity, describe your geographic coverage	
a. Local	
b. Regional	
c. National	
d. International	P
3. Please check the following features your service provides	
a. Filtered searches	P
b. White list (pre-selected content)	P
c. Human Monitored chatrooms	P
d. Technology monitored chatrooms	P
e. Tamper-proof network	P
f. Proprietary Content	P
g. Usage monitoring	P
h. Web hosting	
4. Are your content policies for Internet content consistent for	
a. Web sites you host	P
b. Advertising (banner ads, etc.)	P
c. Newsgroup feeds	P
5. How do you offer your service?	
a. Dial up (What speeds)	P
b. T-1 access	P
c. DSL	P
d. Broadband	P
6. Your service is compatible with a third party's	
a. Dial up (What speeds)	P
b. T-1 access	P
c. DSL	P
d. Broadband	P

C. FOR CLIENT SIDE APPLICATIONS	
1. Regarding product updates, does your product	
a. Automatically updates itself?	
b. Customer must download updates	P
c. Other	
2. Do these updates cost anything?	
a. Free	P
b. $1 - $25	
c. $26 - $50	
d. $51 - $100	

	Anti-Defamation League Hatefilter (ADL)	Awesome Library Website (EDI)
e. Greater than $100		
3. If your company does automatic updates, how often are updates done?		
a. Daily		
b. Weekly		P
c. Monthly		
d. As needed	P	

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling and Rating Technologies

	BASCOM Global Internet	Chaperon 2000
e Greater than $100		
3 If your company does automatic updates, how often are updates done?		
a Daily	P	
b Weekly		
c Monthly		
d As needed		

	Characterlink	**Childwatch by PACEL Corporation**
e Greater than $100		
3 If your company does automatic updates, how often are updates done?		
a Daily		
b Weekly		P
c Monthly		
d As needed		

990

991

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling, and Rating Technologies

	Cyber Patrol	Cyber Sentinel V2.0
e. Greater than $100		
3. If your company does automatic updates, how often are updates done?		
a. Daily	P	
b. Weekly		
c. Monthly		
d. As needed		P

	CYBERsitter 2000	**Desktop Surveillance**
e Greater than $100		
3. If your company does automatic updates, how often are updates done?		N/A
a Daily		
b Weekly	P	
c Monthly		
d As needed		

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling and Rating Technologies

	Digimarc Corporation	Dotsafe, Inc.
e. Greater than $100		
3. If your company does automatic updates, how often are updates done?		
a. Daily		
b. Weekly		
c. Monthly		
d. As needed		

	E-Junk, Obvious Solutions	**FamilyClick.com, LLC**	**FamilyConnect**
e. Greater than $100	P		
3. If your company does automatic updates, how often are updates done?			
a. Daily			
b. Weekly	P		
c. Monthly			
d. As needed			

998

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling and Rating Technologies

	iForAll	Integrity Online	Integrity Online
e. Greater than $100			
3. If your company does automatic updates, how often are updates done?			
a. Daily			P
b. Weekly			
c. Monthly			
d. As needed			

	Internet Safari, by	ITECH INC.
e. Greater than $100		
3. If your company does automatic updates, how often are updates done?		
a. Daily		
b. Weekly		
c. Monthly		
d. As needed		

	Microsoft IE5 Content Advisor
e. Greater than $100	
3. If your company does automatic updates, how often are updates done?	
a. Daily	
b. Weekly	
c. Monthly	
d. As needed	

Commission on Online Child Protection (Filtering Evaluation)

Request for Information and Submissions by Vendors/Operators of Current Filtering, Labeling and Rating Technologies

	N2H2
e. Greater than $100	
3. If your company does automatic updates, how often are updates done?	
a. Daily	
b. Weekly	
c. Monthly	
d. As needed	

	Net Nanny Software, Inc.	PlanetGood Technologies, Inc.
e. Greater than $100		
3. If your company does automatic updates, how often are updates done?		N/A
a. Daily		
b. Weekly		
c. Monthly		
d. As needed		

	REALTIME SENTRY	RSACi, Internet Content Rating Services/
e. Greater than $100		
3. If your company does automatic updates, how often are updates done?		
a. Daily		
b. Weekly		
c. Monthly		
d. As needed	P	

	Safe Access	**SafeSurf Internet Filtering Solution**
e. Greater than $100		
3. If your company does automatic updates, how often are updates done?		
a. Daily		
b. Weekly		
c. Monthly		
d. As needed		

	Safexplorer	Stanford University	WinGuardian
e. Greater than $100			
3. If your company does automatic updates, how often are updates done?			
a. Daily			
b. Weekly			
c. Monthly			
d. As needed	P		

	XSTOP.com R2000	Yahoo!
e. Greater than $100		
3. If your company does automatic updates, how often are updates done?		
a. Daily	P	
b. Weekly		
c. Monthly		
d. As needed		

	Zeek Safe (Zeeks.com, Inc.)
e. Greater than $100	
3. If your company does automatic updates, how often are updates done?	N/A
a. Daily	
b. Weekly	
c. Monthly	
d. As needed	

COPA Commissioners Questionnaire Responses

Common Resources and Parental Education

1. Online information resources

Collection of information regarding technologies and methods that can protect children and publication of such information on an open web page, with links to additional pertinent materials.

The Commission rated each technology/method in light of both its current effectiveness and near-term potential effectiveness, relative to other technologies and methods, in reducing access by children to harmful to minor's materials (when used along with other related technologies and methods).

(note special features of "one click away" approach)

a. How effective is this Technology/Method in preventing access by children to harmful to minor's material (on a scale of 0-10, with 0 being ineffective and 10 being completely effective)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (5)
Bastian (1)
Berman (5)
DeRosier (1)
Flores (5)
Ganier (1)
Hughes (2
Parker (2)
Schmidt (2)
Schrader (8)
Shapiro (6)
Srinivasan (7)
Talbert (1)
Telage (4)
Vradenburg (5)

b. How accessible is this Technology/Method (easy to find, implement and use) (on a scale of 0-10, with 0 being totally inaccessible and 10 being totally accessible)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (5)
Bastian (7)
Berman (8)
DeRosier (6)
Flores (3)
Ganier (4)
Hughes (5)
Parker (6)
Schmidt (10)
Schrader (9)
Shapiro (9)
Srinivasan (8)
Talbert (5)
Telage (6)

Vradenburg (9)

c. How costly is this Technology/Method to users (considering direct and indirect costs) (on a scale of 0-10, with 0 being free and 10 being very expensive)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (1)
Bastian (0)
Berman (0)
DeRosier (2) – The costs get passed on.
Flores (1)
Ganier (2)
Hughes (1)
Parker (0)
Schmidt (0)
Schrader (0)
Shapiro (0)
Srinivasan (2)
Talbert (0)
Telage (2)
Vradenburg (1)

d. How costly is this Technology/Method to sources of otherwise lawful adult content that would be deemed harmful to minors under COPA, (considering direct and indirect costs) (on a scale of 0-10, with 0 being free and 10 being very expensive)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (0)
Bastian (1)
Berman (0)
DeRosier (1)
Flores (0)
Ganier (0)
Hughes (0)
Parker (0)
Schmidt (3)
Schrader (1)
Shapiro (3)
Srinivasan (0)
Talbert (0)
Telage (0)
Vradenburg (3)

e. How extensive are the adverse impacts of this technology on privacy (on a scale of 0-10, with 0 meaning no adverse impacts and 10 meaning very substantial adverse impacts)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (0)
Bastian (0)
Berman (1)
DeRosier (1)
Flores (0)
Ganier (0)
Hughes (0)
Parker (0)
Schmidt (0)

Schrader (0)
Shapiro (0)
Srinivasan (0)
Talbert (0)
Telage (1)
Vradenburg (0)

f. How extensive are the adverse impacts of this technology on first amendment values (protection of lawful adult speech) (on a scale of 0-10, with 0 meaning no adverse impacts and 10 meaning very substantial adverse impacts)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (0)
Bastian (0)
Berman (2)
DeRosier (1)
Flores (1)
Ganier (1)
Hughes (0)
Parker (0)
Schmidt (0)
Schrader (1)
Shapiro (0)
Srinivasan (0)
Talbert (0)
Telage (1)
Vradenburg (0)

g. How extensive are the adverse impacts of this technology on law enforcement (on a scale of 0-10, with 0 meaning no adverse impacts, and 10 meaning very substantial adverse impacts)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (0)
Bastian (0)
Berman (0)
DeRosier (1)
Flores (NA)
Ganier (1)
Hughes (+)
Parker (0)
Schmidt (0)
Schrader (0)
Shapiro (0)
Srinivasan (0)
Talbert (0)
Telage (1)
Vradenburg (0)

2. Parent Education Programs

Active outreach to educate families about both opportunities and dangers of the internet, as well as the tools and practices that can optimize a child's experience online -- with a goal of encouraging parents' involvement with their children's online experience and wider adoption of common sense practices.

a. How effective is this Technology/Method in preventing access by children to harmful to minor's material (on a scale of 0-10, with 0 being ineffective and 10 being completely effective)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (8)
Bastian (2)
Berman (8)
DeRosier (5)
Flores (5)
Ganier (2)
Hughes (4)
Parker (3)
Schmidt (2)
Schrader (6)
Shapiro (8)
Srinivasan (8)
Talbert (5)
Telage (4)
Vradenburg (8)

b. How accessible is this Technology/Method (easy to find, implement and use) (on a scale of 0-10, with 0 being totally inaccessible and 10 being totally accessible)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (7)
Bastian (7)
Berman (8)
DeRosier (5)
Flores (2)
Ganier (2)
Hughes (6)
Parker (4)
Schmidt (8)
Schrader (9)
Shapiro (8)
Srinivasan (4)
Talbert (5)
Telage (4)
Vradenburg (4)

c. How costly is this Technology/Method to users (considering direct and indirect costs) (on a scale of 0-10, with 0 being free and 10 being very expensive)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (2)
Bastian (0)

Berman (1)
DeRosier (1)
Flores (1)
Ganier (1).
Hughes (1)
Parker (0)
Schmidt (6)
Schrader (2)
Shapiro (0)
Srinivasan (2)
Talbert (2)
Telage (2)
Vradenburg (0)

d. How costly is this Technology/Method to sources of otherwise lawful adult content that would be deemed harmful to minors under COPA (considering direct and indirect costs) (on a scale of 0-10, with 0 being free and 10 being very expensive)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (1)
Bastian (0)
Berman (1)
DeRosier (1)
Flores (1)
Ganier (1)
Hughes (0)
Parker (1)
Schmidt (1)
Schrader (0)
Shapiro (3)
Srinivasan (0)
Talbert (1)
Telage (1)
Vradenburg (3)

e. How extensive are the adverse impacts of this technology on privacy (on a scale of 0-10, with 0 meaning no adverse impacts and 10 meaning very substantial adverse impacts)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (0)
Bastian (0)
Berman (0)
DeRosier (1)
Flores (0)
Ganier (0)
Hughes (0)
Parker (0)
Schmidt (0)
Schrader (0)
Shapiro (0)
Srinivasan (0)
Talbert (0)
Telage (1)
Vradenburg (0)

f. How extensive are the adverse impacts of this technology on first amendment values (protection of lawful adult speech) (on a scale of 0-10, with 0 meaning no adverse impacts and 10 meaning very substantial adverse impacts)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (0)
Bastian (0)
Berman (0)
DeRosier (1)
Flores (0)
Ganier (0)
Hughes (0)
Parker (0)
Schmidt (0)
Schrader (1)
Shapiro (0)
Srinivasan (0)
Talbert (0)
Telage (1)
Vradenburg (0)

g. How extensive are the adverse impacts of this technology on law enforcement (on a scale of 0-10, with 0 meaning no adverse impacts, and 10 meaning very substantial adverse impacts)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (0)
Bastian (0)
Berman (0)
DeRosier (0)
Flores (0)
Ganier (0)
Hughes (+)
Parker (0)
Schmidt (0)
Schrader (0)
Shapiro (0)
Srinivasan (0)
Talbert (0)
Telage (0)
Vradenburg (0)

Filtering/Blocking

3. Server-side filtering using URL lists

Voluntary use by Internet Service Providers and Online Services of server software that denies access to particular content sources (identified by uniform resource locators) that have been selected for blocking. The selection of the blocked list can rely upon automated processes, human review, and user options. The list of blocked URLs may or may not be disclosed. The list is regularly updated at the server.

a. How effective is this Technology/Method in preventing access by children to harmful to minor's material (on a scale of 0-10, with 0 being ineffective and 10 being completely effective)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (7)
Bastian (6)
Berman (7)
DeRosier (7)
Flores (9)
Ganier (7)
Hughes (9)
Parker (9)
Schmidt (6)
Schrader (8)
Shapiro (7)
Srinivasan (8)
Talbert (7)
Telage (7)
Vradenburg (7)

b. How accessible is this Technology/Method (easy to find, implement and use) (on a scale of 0-10, with 0 being totally inaccessible and 10 being totally accessible)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (7)
Bastian (7)
Berman (2)
DeRosier (5)
Flores (7)
Ganier (school 7, home 3)
Hughes (8)
Parker (6)
Schmidt (9)
Schrader (8) – Server-side filtering is obviously easier to use than client-side systems.
Shapiro (5)
Srinivasan (8)
Talbert (5) – Fairly easy to find but implementation and use varies with different types of technologies. Some services are incompatible or difficult to implement with some software/hardware configurations and most require the user to have basic skills that some parents may lack in trying to load a program.
Telage (7)
Vradenburg (9)

c. How costly is this Technology/Method to users (considering direct and indirect costs) (on a scale of 0-10, with 0 being free and 10 being very expensive)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (1)
Bastian (5)
Berman (5)
DeRosier (4)
Flores (4)
Ganier (5)
Hughes (2)
Parker (6)
Schmidt (1)
Schrader (2)
Shapiro (4)
Srinivasan (5)
Talbert (3)
Telage (5)
Vradenburg (4)

d. How costly is this Technology/Method to sources of otherwise lawful adult content that would be deemed harmful to minors under COPA (considering direct and indirect costs) (on a scale of 0-10, with 0 being free and 10 being very expensive)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (1)
Bastian (0)
Berman (0)
DeRosier (4)
Flores (0)
Ganier (1)
Hughes (0)
Parker (0)
Schmidt (1)
Schrader (0)
Shapiro (2)
Srinivasan (0)
Talbert (0)
Telage (0)
Vradenburg (0)

e. How extensive are the adverse impacts of this technology on privacy (on a scale of 0-10, with 0 meaning no adverse impacts and 10 meaning very substantial adverse impacts)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (3)
Bastian (3)
Berman (5)
DeRosier (0)
Flores (1)
Ganier (2)
Hughes (1)
Parker (0)
Schmidt (1)
Schrader (4)
Shapiro (2)

Srinvasan (2)
Talbert (3)
Telage (3)
Vradenburg (2)

f. How extensive are the adverse impacts of this technology on first amendment values (protection of lawful adult speech) (on a scale of 0-10, with 0 meaning no adverse impacts and 10 meaning very substantial adverse impacts)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (4)
Bastian (5)
Berman (8)
DeRosier (5)
Flores (1)
Ganier (2)
Hughes (1)
Parker (3)
Schmidt (9)
Schrader (5)
Shapiro (4)
Srinivasan (3)
Talbert (1)
Telage (5)
Vradenburg (3)

g. How extensive are the adverse impacts of this technology on law enforcement (on a scale of 0-10, with 0 meaning no adverse impacts, and 10 meaning very substantial adverse impacts)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (0)
Bastian (0)
Berman (0)
DeRosier (0)
Flores (0)
Ganier (0)
Hughes (+)
Parker (0)
Schmidt (1)
Schrader (0)
Shapiro (0)
Srinivasan (0)
Talbert (0)
Telage (3)
Vradenburg (0)

---

4. Client-side filtering using URL lists

Voluntary use by end users of software that causes the browser not to download content from specified content sources. The list of blocked sites may originate from both the software supplier and/or from decisions by the user. The list may be updated periodically by means of a download from the site of the software provider. The list may or may not be disclosed. A denial of access may be overridden with the use of a password controlled by a parent. The PC-based software may also filter out email or instant messaging from unapproved sources.

a. How effective is this Technology/Method in preventing access by children to harmful to minor's material (on a scale of 0-10, with 0 being ineffective and 10 being completely effective)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (6)
Bastian (8)
Berman (8)
DeRosier (5)
Flores (8)
Ganier (5)
Hughes (7)
Parker (8)
Schmidt (6)
Schrader (9)
Shapiro (6)
Srinivasan (9)
Talbert (4)
Telage (5)
Vradenburg (4)

b. How accessible is this Technology/Method (easy to find, implement and use) (on a scale of 0-10, with 0 being totally inaccessible and 10 being totally accessible)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (5)
Bastian (8)
Berman (8)
DeRosier (5)
Flores (8)
Ganier (3)
Hughes (6)
Parker (6)
Schmidt (9)
Schrader (7)
Shapiro (7)
Srinivasan (8)
Talbert (8)
Telage (7)
Vradenburg (8)

c. How costly is this Technology/Method to users (considering direct and indirect costs) (on a scale of 0-10, with 0 being free and 10 being very expensive)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (3)
Bastian (5)
Berman (3)
DeRosier (3)
Flores (5)
Ganier (8)
Hughes (5)
Parker (6)
Schmidt (5)
Schrader (3)
Shapiro (4)
Srinivasan (5)
Talbert (3)
Telage (5)
Vradenburg (3)

d. How costly is this Technology/Method to sources of otherwise lawful adult content that would be deemed harmful to minors under COPA (considering direct and indirect costs) (on a scale of 0-10, with 0 being free and 10 being very expensive)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (0)
Bastian (0)
Berman (2)
DeRosier (1)
Flores (0)
Ganier (0)
Hughes (0)
Parker (0)
Schmidt (1)
Schrader (0)
Shapiro (0)
Srinivasan (0)
Talbert (0)
Telage (0)
Vradenburg (0)

e. How extensive are the adverse impacts of this technology on privacy (on a scale of 0-10, with 0 meaning no adverse impacts and 10 meaning very substantial adverse impacts)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (3)
Bastian (2)
Berman (3)
DeRosier (0)
Flores (1)
Ganier (2)
Hughes (1)
Parker (0)
Schmidt (4)
Schrader (3)
Shapiro (1)
Srinivasan (0)
Talbert (0)
Telage (3)
Vradenburg (2)

f. How extensive are the adverse impacts of this technology on first amendment values (protection of lawful adult speech) (on a scale of 0-10, with 0 meaning no adverse impacts and 10 meaning very substantial adverse impacts)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (5)
Bastian (0)
Berman (4)
DeRosier (0)
Flores (0)
Ganier (1)
Hughes (1)
Parker (1)
Schmidt (2)
Schrader (2)
Shapiro (3)
Srinivasan (3)
Talbert (1)
Telage (3)
Vradenburg (5)

g. How extensive are the adverse impacts of this technology on law enforcement (on a scale of 0-10, with 0 meaning no adverse impacts, and 10 meaning very substantial adverse impacts)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (0)
Bastian (0)
Berman (0)
DeRosier (0)
Flores (0)
Ganier (2)
Hughes (0)
Parker (0)
Schmidt (1)
Schrader (0)
Shapiro (0)
Srinivasan (0)
Talbert (0)
Telage (0)
Vradenburg (0)

---

5. Filtering (server- and client-side) using content analysis

Voluntary use of some combination of PC-based software and server software that conducts (when necessary) real time analysis of the content of a web site and filters out content sources that fit some algorithm. Such a system may be able to deal with pictures as well as words and may be able to analyze email and attachments. The end user may or may not be informed of the nature of the algorithm and may or may not have full information regarding what is being excluded.

The Commission limited discussion of this to systems using real time analysis of text. (picture analysis moved to other section)

a. How effective is this Technology/Method in preventing access by children to harmful to minor's material (on a scale of 0-10, with 0 being ineffective and 10 being completely effective)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (5)
Bastian (7)
Berman (5)
DeRosier (5)
Flores – (7)
Ganier (2)
Hughes (10)
Parker (7)
Schmidt (Unknown)
Schrader (4)
Shapiro (2)
Srinivasan (8)
Talbert (7)
Telage (2)
Vradenburg (4)

b. How accessible is this Technology/Method (easy to find, implement and use) (on a scale of 0-10, with 0 being totally inaccessible and 10 being totally accessible)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (2)
Bastian (2)
Berman (3)
DeRosier (5)
Flores (2)
Ganier (2)
Hughes (2)
Parker (7)
Schmidt (Unknown)
Schrader (3)
Shapiro (3)
Srinivasan (5)
Talbert (5)
Telage (3)
Vradenburg (1)

c. How costly is this Technology/Method to users (considering direct and indirect costs) (on a scale of 0-10, with 0 being free and 10 being very expensive)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (5)
Bastian (5)
Berman (3)
DeRosier (3)
Flores (4)
Ganier (7)
Hughes (0)
Parker (7)
Schmidt (5)
Schrader (2)
Shapiro (5)
Srinivasan (5)
Talbert (5)
Telage (6)
Vradenburg (6)

d. How costly is this Technology/Method to sources of otherwise lawful adult content that would be deemed harmful to minors under COPA (considering direct and indirect costs) (on a scale of 0-10, with 0 being free and 10 being very expensive)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (1)
Bastian (0)
Berman (0)
DeRosier (1)
Flores (1)
Ganier (1)
Hughes (0)
Parker (0)
Schmidt (2)
Schrader (0)
Shapiro (1)

Srinivasan (0)
Talbert (0)
Telage (0)
Vradenburg (0)

e. How extensive are the adverse impacts of this technology on privacy (on a scale of 0-10, with 0 meaning no adverse impacts and 10 meaning very substantial adverse impacts)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (3)
Bastian (3)
Berman (4)
DeRosier (1)
Flores (2)
Ganier (2)
Hughes (0)
Parker (0)
Schmidt (1)
Schrader (3)
Shapiro (3)
Srinivasan (1)
Talbert (3)
Telage (5)
Vradenburg (2)

f. How extensive are the adverse impacts of this technology on first amendment values (protection of lawful adult speech) (on a scale of 0-10, with 0 meaning no adverse impacts and 10 meaning very substantial adverse impacts)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (4)
Bastian (3)
Berman (4)
DeRosier (1)
Flores (2-3)
Ganier (2)
Hughes (2)
Parker (3)
Schmidt (8)
Schrader (4)
Shapiro (4)
Srinivasan (3)
Talbert (3)
Telage (5)
Vradenburg (5)

g. How extensive are the adverse impacts of this technology on law enforcement (on a scale of 0-10, with 0 meaning no adverse impacts, and 10 meaning very substantial adverse impacts)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (0)
Bastian (0)
Berman (0)
DeRosier (1)
Flores (0)
Ganier (1)

Hughes (0)
Parker (0)
Schmidt (1)
Schrader (0)
Shapiro (0)
Srinivasan (0)
Talbert (0)
Telage (0)
Vradenburg (0)

Labeling and Rating Systems

6. First-party labeling/rating

Voluntary action by content sources to indicate that a site or particular content meets a particular standard or fits a particular category. The "label" can take the form of a metatag, or entry into a database listing, or display of a seal. The use of a label may be audited. For purposes of considering this technology, the Commission will assume that the voluntary labeling scheme would identify material that is "Harmful to Minors" and thereby allow others to filter or block such material.

a. How effective is this Technology/Method in preventing access by children to harmful to minor's material (on a scale of 0-10, with 0 being ineffective and 10 being completely effective)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (8)
Bastian (7)
Berman (5)
DeRosier (4)
Flores (5)
Ganier (2)
Hughes (4)
Parker (8)
Schmidt (4)
Schrader (4)
Shapiro (4)
Srinivasan (8)
Talbert (5)
Telage (8)
Vradenburg (3)

b. How accessible is this Technology/Method (easy to find, implement and use) (on a scale of 0-10, with 0 being totally inaccessible and 10 being totally accessible)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (5)
Bastian (4)
Berman (3)
DeRosier (6)
Flores (4)
Ganier (2)
Hughes (4)
Parker (8)
Schmidt (8)
Schrader (6)
Shapiro (4)
Srinivasan (8)
Talbert (4)
Telage (5)
Vradenburg (5)

c. How costly is this Technology/Method to users (considering direct and indirect costs) (on a scale of 0-10, with 0 being free and 10 being very expensive)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (0)
Bastian (1)
Berman (3)
DeRosier (2)
Flores (1)
Ganier (1)
Hughes (1)
Parker (2)
Schmidt (1)
Schrader (1)
Shapiro (1)
Srinivasan (0)
Talbert (2)
Telage (2)
Vradenburg (0)

d. How costly is this Technology/Method to sources of otherwise lawful adult content that would be deemed harmful to minors under COPA (considering direct and indirect costs) (on a scale of 0-10, with 0 being free and 10 being very expensive)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (2)
Bastian (5)
Berman (6)
DeRosier (4)
Flores (5)
Ganier (3)
Hughes (2)
Parker (3)
Schmidt (7)
Schrader (8)
Shapiro (6)
Srinivasan (4
Talbert (2)
Telage (5)
Vradenburg (5)

e. How extensive are the adverse impacts of this technology on privacy (on a scale of 0-10, with 0 meaning no adverse impacts and 10 meaning very substantial adverse impacts)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (0)
Bastian (0)
Berman (2)
DeRosier (0)
Flores (0)
Ganier (1)
Hughes (0)
Parker (0)
Schmidt (1)
Schrader (3)
Shapiro (2)
Srinivasan (0)
Talbert (0)
Telage (3)

Vradenburg (0)

f. How extensive are the adverse impacts of this technology on first amendment values (protection of lawful adult speech) (on a scale of 0-10, with 0 meaning no adverse impacts and 10 meaning very substantial adverse impacts)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (1)
Bastian (0)
Berman (5)
DeRosier (3)
Flores (2)
Ganier (1)
Hughes (1)
Parker (2)
Schmidt (8)
Schrader (5)
Shapiro (2)
Srinivasan (3
Talbert (1)
Telage (3)
Vradenburg (5)

g. How extensive are the adverse impacts of this technology on law enforcement (on a scale of 0-10, with 0 meaning no adverse impacts, and 10 meaning very substantial adverse impacts)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (0)
Bastian (1)
Berman (0)
DeRosier (0)
Flores (0)
Ganier (1)
Hughes (0)
Parker (0)
Schmidt (1)
Schrader (0)
Shapiro (0)
Srinivasan (0)
Talbert (0)
Telage (1)
Vradenburg (0)

7. Third-party labeling/rating

Voluntary action by third parties to review content sources and to associate labels or ratings with such sources so as to enable filtering or blocking by others. The review may involve some automated parsing and some human judgment. For purposes of considering this technology, the Commission will assume that the labeling and related filtering may involve various "categories" established by private parties and that no affirmative action is required by a content source.

a. How effective is this Technology/Method in preventing access by children to harmful to minor's material (on a scale of 0-10, with 0 being ineffective and 10 being completely effective)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (3)
Bastian (3)
Berman (3)
DeRosier (3)
Flores (0)
Ganier (4)
Hughes (3)
Parker (4)
Schmidt (2)
Schrader (5)
Shapiro (2)
Srinivasan (4)
Talbert (2)
Telage (3) (4)
Vradenburg (1)

b. How accessible is this Technology/Method (easy to find, implement and use) (on a scale of 0-10, with 0 being totally inaccessible and 10 being totally accessible)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (3)
Bastian (3)
Berman (3)
DeRosier (6)
Flores (4)
Ganier (3)
Hughes (3)
Parker (4)
Schmidt (8)
Schrader (4)
Shapiro (2)
Srinivasan (4)
Talbert (1)
Telage (3)
Vradenburg (1)

c. How costly is this Technology/Method to users (considering direct and indirect costs) (on a scale of 0-10, with 0 being free and 10 being very expensive)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (1)
Bastian (1)

Berman (3)
DeRosier (2)
Flores (4)
Ganier (3)
Hughes (1)
Parker (2)
Schmidt (1)
Schrader (1)
Shapiro (0)
Srinivasan (0)
Talbert (2)
Telage (5)
Vradenburg (0)

d. How costly is this Technology/Method to sources of otherwise lawful adult content that would be deemed harmful to minors under COPA (considering direct and indirect costs) (on a scale of 0-10, with 0 being free and 10 being very expensive)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (0)
Bastian (0)
Berman (0)
DeRosier (2)
Flores (0)
Ganier (1)
Hughes (0)
Parker (1)
Schmidt (1)
Schrader (1)
Shapiro (3)
Srinivasan (0)
Talbert (2)
Telage (0)
Vradenburg (0)

e. How extensive are the adverse impacts of this technology on privacy (on a scale of 0-10, with 0 meaning no adverse impacts and 10 meaning very substantial adverse impacts)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (0)
Bastian (0)
Berman (1)
DeRosier (0)
Flores (0)
Ganier (1)
Hughes (0)
Parker (0)
Schmidt (1)
Schrader (0)
Shapiro (1)
Srinivasan (0)
Talbert (0)
Telage (2)
Vradenburg (0)

f. How extensive are the adverse impacts of this technology on first amendment values (protection of lawful adult speech) (on a scale of 0-10, with 0 meaning no adverse impacts and 10 meaning very substantial adverse impacts)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (5)
Bastian (3)
Berman (3)
DeRosier (3)
Flores (0)
Ganier (1)
Hughes (0)
Parker (2)
Schmidt (7)
Schrader (6)
Shapiro (3)
Srinivasan (3)
Talbert (3)
Telage (3)
Vradenburg (5)

g. How extensive are the adverse impacts of this technology on law enforcement (on a scale of 0-10, with 0 meaning no adverse impacts, and 10 meaning very substantial adverse impacts)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (0)
Bastian (0)
Berman (0)
DeRosier (0)
Flores (0)
Ganier (1)
Hughes (0)
Parker (0)
Schmidt (1)
Schrader (0)
Shapiro (0)
Srinivasan (0)
Talbert (0)
Telage (1)
Vradenburg (0)

Age Verification Systems

8. AVS based on credit cards

Use by a content source of a system to condition access to a web page (or pushed content) on the end user's ability to provide a credit card number. The number may or may not be verified as relating to a valid card (it may not be used for charging a fee) and may or may not be further analyzed to assure that the holder of the card is an adult.

a. How effective is this Technology/Method in preventing access by children to harmful to minor's material (on a scale of 0-10, with 0 being ineffective and 10 being completely effective)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (3)
Bastian (5)
Berman (4)
DeRosier (7)
Flores (9)
Ganier (2)
Hughes (9+)
Parker (8)
Schmidt (2)
Schrader (2)
Shapiro (7)
Srinivasan (8)
Talbert (5)
Telage (5)
Vradenburg (7)

b. How accessible is this Technology/Method (easy to find, implement and use) (on a scale of 0-10, with 0 being totally inaccessible and 10 being totally accessible)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (3)
Bastian (8)
Berman (4)
DeRosier (9)
Flores (8)
Ganier (7)
Hughes (8)
Parker (8)
Schmidt (8)
Schrader (5)
Shapiro (8)
Srinivasan (9)
Talbert (8)
Telage (7)
Vradenburg (8)

c. How costly is this Technology/Method to users (considering direct and indirect costs) (on a scale of 0-10, with 0 being free and 10 being very expensive)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (5)
Bastian (1)
Berman (4)
DeRosier (3)
Flores (1)
Ganier (2)
Hughes (1)
Parker (1)
Schmidt (6)
Schrader (8) -- Being required to use a credit card to access HTM sites or specific HTM content is, at the very least, burdensome and discouraging to adults, and in many cases, an absolute bar to receiving lawful speech on the Internet (since a significant percentage of adults do not have credit cards).
Shapiro (5)
Srinivasan (1)
Talbert (1)
Telage (3)
Vradenburg (2)

d. How costly is this Technology/Method to sources of otherwise lawful adult content that would be deemed harmful to minors under COPA (considering direct and indirect costs) (on a scale of 0-10, with 0 being free and 10 being very expensive)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (8)
Bastian (6)
Berman (6)
DeRosier (3)
Flores (2)
Ganier (10)
Hughes (2)
Parker (5)
Schmidt (1)
Schrader (8)
Shapiro (6)
Srinivasan (9)
Talbert (4)
Telage (8)
Vradenburg (8)

e. How extensive are the adverse impacts of this technology on privacy (on a scale of 0-10, with 0 meaning no adverse impacts and 10 meaning very substantial adverse impacts)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (5)
Bastian (3)
Berman (6)
DeRosier (4)
Flores (3)
Ganier (10)
Hughes (2)
Parker (5)
Schmidt (6)
Schrader (10)
Shapiro (5)
Srinivasan (2)

Talbert (4)
Telage (8)
Vradenburg (5)

f. How extensive are the adverse impacts of this technology on first amendment values (protection of lawful adult speech) (on a scale of 0-10, with 0 meaning no adverse impacts and 10 meaning very substantial adverse impacts)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (5)
Bastian (3)
Berman (7)
DeRosier (2)
Flores (2)
Ganier (6)
Hughes (2)
Parker (2)
Schmidt (2)
Schrader (8)
Shapiro (8)
Srinivasan (2)
Talbert (2)
Telage (8)
Vradenburg (8)

g. How extensive are the adverse impacts of this technology on law enforcement (on a scale of 0-10, with 0 meaning no adverse impacts, and 10 meaning very substantial adverse impacts)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (3)
Bastian (1)
Berman (2)
DeRosier (1)
Flores (0)
Ganier (3)
Hughes (+)
Parker (0)
Schmidt (1)
Schrader (0)
Shapiro (0)
Srinivasan (0)
Talbert (1)
Telage (3)
Vradenburg (0)

9. AVS based on independently-issued ID

Use by a content source of a system to condition access to a web page (or pushed content) on the end user's use of a password protected identifier that is issued (by a third party) only to those who have presented some credentials indicating adult age.

a. How effective is this Technology/Method in preventing access by children to harmful to minor's material (on a scale of 0-10, with 0 being ineffective and 10 being completely effective)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (3)
Bastian (5)
Berman (3)
DeRosier (5)
Flores (9)
Ganier (2)
Hughes (9+)
Parker (8)
Schmidt (8)
Schrader (3)
Shapiro (8)
Srinivasan (8)
Talbert (3)
Telage (6)
Vradenburg (9)

b. How accessible is this Technology/Method (easy to find, implement and use) (on a scale of 0-10, with 0 being totally inaccessible and 10 being totally accessible)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (2)
Bastian (1)
Berman (3)
DeRosier (5)
Flores (8)
Ganier (1)
Hughes (6)
Parker (2)
Schmidt (3)
Schrader (4)
Shapiro (3)
Srinivasan (5)
Talbert (2)
Telage (4)
Vradenburg (8)

c. How costly is this Technology/Method to users (considering direct and indirect costs) (on a scale of 0-10, with 0 being free and 1 0 being very expensive)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (6)
Bastian (3)
Berman (5)
DeRosier (2)

Flores (1)
Ganier (7)
Hughes (2)
Parker (3)
Schmidt (2)
Schrader (8)
Shapiro (5)
Srinivasan (2)
Talbert (4)
Telage (5)
Vradenburg (7)

d. How costly is this Technology/Method to sources of otherwise lawful adult content that would be deemed harmful to minors under COPA (considering direct and indirect costs) (on a scale of 0-10, with 0 being free and 10 being very expensive)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (8)
Bastian (6)
Berman (5)
DeRosier (2)
Flores (1)
Ganier (8)
Hughes (1)
Parker (6)
Schmidt (3)
Schrader (7)
Shapiro (8)
Srinivasan (7)
Talbert (8)
Telage (8)
Vradenburg (8)

e. How extensive are the adverse impacts of this technology on privacy (on a scale of 0-10, with 0 meaning no adverse impacts and 10 meaning very substantial adverse impacts)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (5)
Bastian (6)
Berman (5)
DeRosier (5)
Flores (1)
Ganier (10)
Hughes (2)
Parker (5)
Schmidt (5)
Schrader (9)
Shapiro (5)
Srinivasan (0)
Talbert (5)
Telage (8)
Vradenburg (5)

f. How extensive are the adverse impacts of this technology on first amendment values (protection of lawful adult speech) (on a scale of 0-10, with 0 meaning no adverse impacts and 10 meaning very substantial adverse impacts)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (6)
Bastian (9)
Berman (8)
DeRosier (6)
Flores (3)
Ganier (6)
Hughes (3+)
Parker (2)
Schmidt (3)
Schrader (9)
Shapiro (8)
Srinivasan (0)
Talbert (3)
Telage (9)
Vradenburg (9)

g. How extensive are the adverse impacts of this technology on law enforcement (on a scale of 0-10, with 0 meaning no adverse impacts, and 10 meaning very substantial adverse impacts)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (2)
Bastian (0)
Berman (1)
DeRosier (3)
Flores (0)
Ganier (3)
Hughes (+)
Parker (0)
Schmidt (2)
Schrader (0)
Shapiro (0)
Srinivasan (0)
Talbert (3)
Telage (3)
Vradenburg (0)

New Top-Level Domain/Zoning

10. Establishment of a gTLD for HTM content

Creation for voluntary use of a new top level domain (e.g., .xxx or .adult) the use of which would be understood to signify that materials on web pages located in such domain (and email coming from such domain) are harmful to minors materials -- and the existence of which would make it easy for browsers or ISPs to filter out all material so located. In analyzing this technology and method, the Commission will assume that placement of material in such domain, to the exclusion of other domains, would constitute an affirmative defense to a COPA charge. (See recommendations).

(In analyzing this technology and method, the Commission will assume that placement of material in such domain, to the exclusion of other domains, will constitute an affirmative defense to a COPA charge. See recommendations).

a. How effective is this Technology/Method in preventing access by children to harmful to minor's material (on a scale of 0-10, with 0 being ineffective and 10 being completely effective)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (3)
Bastian (3)
Berman (2)
DeRosier (4)
Flores (3)
Ganier (1)
Hughes (5)
Parker (3)
Schmidt (2)
Schrader (2)
Shapiro (2)
Srinivasan (7)
Talbert (3)
Telage (3)
Vradenburg (5)

b. How accessible is this Technology/Method (easy to find, implement and use) (on a scale of 0-10, with 0 being totally inaccessible and 10 being totally accessible)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (5)
Bastian (5)
Berman (5)
DeRosier (9)
Flores (6)
Ganier (8)
Hughes (9)
Parker (5)
Schmidt (4)
Schrader (4)
Shapiro (9)
Srinivasan (9)
Talbert (9)

Telage (9)
Vradenburg (9)

c. How costly is this Technology/Method to users (considering direct and indirect costs) (on a scale of 0-10, with 0 being free and 10 being very expensive)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (3)
Bastian (1)
Berman (5)
DeRosier (3)
Flores (1)
Ganier (2)
Hughes (0)
Parker (0)
Schmidt (1)
Schrader (2)
Shapiro (1)
Srinvasan (0)
Talbert (1)
Telage (3)
Vradenburg (1)

d. How costly is this Technology/Method to sources of otherwise lawful adult content that would be deemed harmful to minors under COPA (considering direct and indirect costs) (on a scale of 0-10, with 0 being free and 10 being very expensive)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (8)
Bastian (6)
Berman (6)
DeRosier (1)
Flores (1)
Ganier (4)
Hughes (2)
Parker (5)
Schmidt (7)
Schrader (6)
Shapiro (6)
Srinivasan (4)
Talbert (5)
Telage (6)
Vradenburg (7)

e. How extensive are the adverse impacts of this technology on privacy (on a scale of 0-10, with 0 meaning no adverse impacts and 10 meaning very substantial adverse impacts)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (2)
Bastian (0)
Berman (4)
DeRosier (3)
Flores (8)
Ganier (5)
Hughes (2)
Parker (0)

Schmidt (1)
Schrader (4)
Shapiro (0)
Srinivasan (0)
Talbert (4)
Telage (4)
Vradenburg (1)

f. How extensive are the adverse impacts of this technology on first amendment values (protection of lawful adult speech) (on a scale of 0-10, with 0 meaning no adverse impacts and 10 meaning very substantial adverse impacts)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (7)
Bastian (2)
Berman (8)
DeRosier (4)
Flores (9)
Ganier (8)
Hughes (2)
Parker (0)
Schmidt (8)
Schrader (8)
Shapiro (7)
Srinvasan (8)
Talbert (0)
Telage (9)
Vradenburg (9)

g. How extensive are the adverse impacts of this technology on law enforcement (on a scale of 0-10, with 0 meaning no adverse impacts, and 10 meaning very substantial adverse impacts)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (3)
Bastian (1)
Berman (8)
DeRosier (7)
Flores (9)
Ganier (0)
Hughes (+)
Parker (5)
Schmidt (1)
Schrader (3)
Shapiro (2)
Srinivasan (0)
Talbert (3)
Telage (8)
Vradenburg (0)

11. Establishment of a gTLD for non-HTM content

Creation for voluntary use of a new top level domain (e.g., .kids) the use of which would be understood to signify that materials on web pages located in such domain (and email coming from such domain) would universally be considered suitable for minors of all ages -- and the existence of which would make it easy for browsers or ISPs to establish "green zone" features that point or accept only to such materials.

a. How effective is this Technology/Method in preventing access by children to harmful to minor's material (on a scale of 0-10, with 0 being ineffective and 10 being completely effective)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (7)
Bastian (7)
Berman (6)
DeRosier (8)
Flores (5)
Ganier (5)
Hughes (8)
Parker (7)
Schmidt (2)
Schrader (8)
Shapiro (8)
Srinivasan (7)
Talbert (8)
Telage (7)
Vradenburg (1)

b. How accessible is this Technology/Method (easy to find, implement and use) (on a scale of 0-10, with 0 being totally inaccessible and 10 being totally accessible)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (8)
Bastian (1)
Berman (5)
DeRosier (7)
Flores (1)
Ganier (8)
Hughes (9)
Parker (7)
Schmidt (8)
Schrader (5)
Shapiro (8)
Srinivasan (9)
Talbert (8)
Telage (9)
Vradenburg (8)

c. How costly is this Technology/Method to users (considering direct and indirect costs) (on a scale of 0-10, with 0 being free and 10 being very expensive)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (2)
Bastian (1)

Berman (5)
DeRosier (5)
Flores (4)
Ganier (2)
Hughes (2)
Parker (0)
Schmidt (1)
Schrader (1)
Shapiro (4)
Srinivasan (0)
Talbert (1)
Telage (5)
Vradenburg (1)

d. How costly is this Technology/Method to sources of otherwise lawful adult content that would be deemed harmful to minors under COPA (considering direct and indirect costs) (on a scale of 0-10, with 0 being free and 10 being very expensive)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (2)
Bastain (5)
Berman (5)
DeRosier (2)
Flores (1)
Ganier (5)
Hughes (2)
Parker (4)
Schmidt (5)
Schrader (4)
Shapiro (9)
Srinivasan (0)
Talbert (5)
Telage (3)
Vradenburg (8)

e. How extensive are the adverse impacts of this technology on privacy (on a scale of 0-10, with 0 meaning no adverse impacts and 10 meaning very substantial adverse impacts)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (0)
Bastian (0)
Berman (1)
DeRosier (1)
Flores (0)
Ganier ((0)
Hughes (0)
Parker (0)
Schmidt (1)
Schrader (3)
Shapiro (0)
Srinivasan (0)
Talbert (2)
Telage (2)
Vradenburg (0)

f. How extensive are the adverse impacts of this technology on first amendment values (protection of lawful adult speech) (on a scale of 0-10, with 0 meaning no adverse impacts and 10 meaning very substantial adverse impacts)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (1)
Bastian (0)
Berman (5)
DeRosier (1)
Flores (0)
Ganier (1)
Hughes (0)
Parker (0)
Schmidt (3)
Schrader (4)
Shapiro (1)
Srinivasan (0)
Talbert (2)
Telage (2)
Vradenburg (0)

g. How extensive are the adverse impacts of this technology on law enforcement (on a scale of 0-10, with 0 meaning no adverse impacts, and 10 meaning very substantial adverse impacts)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (0)
Bastian (0)
Berman (2)
DeRosier (3)
Flores (0)
Ganier (0)
Hughes (0)
Parker (0)
Schmidt (1)
Schrader (0)
Shapiro (0)
Srinivasan (0)
Talbert (0)
Telage (3)
Vradenburg (0)

---

12. Establishment of a "green zone" or "red light zone" by means of allocation of a new set of IP numbers

Creation for voluntary use of a set of IP numbers (in the new IP version 6 protocol, which has not yet been widely implemented) the use of which would be understood to signify that materials on web pages on servers with such IP numbers (or email coming from such servers) would be either non-HTM material or HTM material, respectively. Any material not in such an IP number zone would be considered to be in a "gray zone" and not necessarily either HTM or non-HTM.

a. How effective is this Technology/Method in preventing access by children to harmful to minor's material (on a scale of 0-10, with 0 being ineffective and 10 being completely effective)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (3)
Bastian (5)
Berman (2)
DeRosier (5)
Flores (4)
Ganier (2)
Hughes (2)
Parker (5)
Schmidt (NA)
Schrader (1)
Shapiro (1)
Srinivasan (4)
Talbert (5)
Telage (5)
Vradenburg (1)

b. How accessible is this Technology/Method (easy to find, implement and use) (on a scale of 0-10, with 0 being totally inaccessible and 10 being totally accessible)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (1)
Bastian (0)
Berman (4)
DeRosier (0)
Flores (0)
Ganier (1)
Hughes (NA)
Parker (2)
Schmidt (NA)
Schrader (0)
Shapiro (0)
Srinivasan (3)
Talbert (3)
Telage (0)
Vradenburg (1)

c. How costly is this Technology/Method to users (considering direct and indirect costs) (on a scale of 0-10, with 0 being free and 10 being very expensive)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (5)
Bastian (1)

Berman (5)
DeRosier (4)
Flores (2)
Ganier (2)
Hughes (1-3)
Parker (1)
Schmidt (NA)
Schrader (3)
Shapiro (1)
Srinivasan (0)
Talbert (1)
Telage (7)
Vradenburg (1)

d. How costly is this Technology/Method to sources of otherwise lawful adult content that would be deemed harmful to minors under COPA (considering direct and indirect costs) (on a scale of 0-10, with 0 being free and 10 being very expensive)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (8)
Bastian (3)
Berman (8)
DeRosier (7)
Flores (2)
Ganier (7)
Hughes (2)
Parker (8)
Schmidt (NA)
Schrader (10)
Shapiro (9)
Srinivasan (7)
Talbert (5)
Telage (8)
Vradenburg (9)

e. How extensive are the adverse impacts of this technology on privacy (on a scale of 0-10, with 0 meaning no adverse impacts and 10 meaning very substantial adverse impacts)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (4)
Bastian (0)
Berman (3)
DeRosier (3)
Flores (0)
Ganier (0)
Hughes (0)
Parker (1)
Schmidt (NA)
Schrader (3)
Shapiro (2)
Srinivasan (0)
Talbert (0)
Telage (5)
Vradenburg (0)

f. How extensive are the adverse impacts of this technology on first amendment values (protection of lawful adult speech) (on a scale of 0-10, with 0 meaning no adverse impacts and 10 meaning very substantial adverse impacts)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (5)
Bastian (0)
Berman (8)
DeRosier (8)
Flores (0)
Ganier (8)
Hughes (2)
Parker (2)
Schmidt (NA)
Schrader (8)
Shapiro (8)
Srinivasan (4)
Talbert (0)
Telage (9)
Vradenburg (9)

g. How extensive are the adverse impacts of this technology on law enforcement (on a scale of 0-10, with 0 meaning no adverse impacts, and 10 meaning very substantial adverse impacts)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (0)
Bastian (0)
Berman (0)
DeRosier (1)
Flores (0)
Ganier (3)
Hughes (+)
Parker (0)
Schmidt (0)
Schrader (0)
Shapiro (0)
Srinivasan (0)
Talbert (0)
Telage (0)
Vradenburg (0)

13. Hotlines

Creation of facilities for easy reporting of problems to the parties who can address them (online and telephone). Assumes hotline would bring problems to attention of both relevant government authorities and private sector groups that can act in response. Assumes activity levels in aggregate and general nature of complaints would be made public.

a. How effective is this Technology/Method in preventing access by children to harmful to minor's material (on a scale of 0-10, with 0 being ineffective and 10 being completely effective)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (2)
Bastian (2)
Berman (6)
DeRosier (5)
Flores (2)
Ganier (3)
Hughes (1)
Parker (3)
Schmidt (1)
Schrader (4)
Shapiro (5)
Srinivasan (2)
Talbert (2)
Telage (2)
Vradenburg (5)

b. How accessible is this Technology/Method (easy to find, implement and use) (on a scale of 0-10, with 0 being totally inaccessible and 10 being totally accessible)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (2)
Bastian (5)
Berman (5)
DeRosier (4)
Flores (4)
Ganier (3)
Hughes (5)
Parker (7)
Schmidt (5)
Schrader (5)
Shapiro (5)
Srinivasan (1)
Talbert (0)
Telage (3)
Vradenburg (5)

c. How costly is this Technology/Method to users (considering direct and indirect costs) (on a scale of 0-10, with 0 being free and 10 being very expensive)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (4)
Bastian (1)
Berman (5)
DeRosier (4)

Flores (6)
Ganier (1)
Hughes (0)
Parker (0)
Schmidt (1)
Schrader (2)
Shapiro (1)
Srinivasan (3)
Talbert (0)
Telage (5)
Vradenburg (1)

d. How costly is this Technology/Method to sources of otherwise lawful adult content that would be deemed harmful to minors under COPA (considering direct and indirect costs) (on a scale of 0-10, with 0 being free and 10 being very expensive)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (0)
Bastian (0)
Berman (2)
DeRosier (4)
Flores (0)
Ganier (3)
Hughes (1)
Parker (0)
Schmidt (5)
Schrader (1)
Shapiro (3)
Srinivasan (0)
Talbert (5)
Telage (0)
Vradenburg (8)

e. How extensive are the adverse impacts of this technology on privacy (on a scale of 0-10, with 0 meaning no adverse impacts and 10 meaning very substantial adverse impacts)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (0)
Bastian (0)
Berman (2)
DeRosier (1)
Flores (0)
Ganier (3)
Hughes (0)
Parker (0)
Schmidt (1)
Schrader (3)
Shapiro (0)
Srinivasan (0)
Talbert (0)
Telage (4)
Vradenburg (0)

f. How extensive are the adverse impacts of this technology on first amendment values (protection of lawful adult speech) (on a scale of 0-10, with 0 meaning no adverse impacts and 10 meaning very substantial adverse impacts)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (3)
Bastian (0)
Berman (2)
DeRosier (1)
Flores (0)
Ganier (3)
Hughes (0)
Parker (0)
Schmidt (6)
Schrader (2)
Shapiro (0)
Srinivasan (0)
Talbert (0)
Telage (2)
Vradenburg (2)

g. How extensive are the adverse impacts of this technology on law enforcement (on a scale of 0-10, with 0 meaning no adverse impacts, and 10 meaning very substantial adverse impacts)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (0)
Bastian (0)
Berman (0)
DeRosier (1)
Flores (0)
Ganier (0)
Hughes (0)
Parker (0)
Schmidt (1)
Schrader (0)
Shapiro (0)
Srinivasan (0)
Talbert (0)
Telage (0)
Vradenburg (0)

Other Technologies and Methods

14. Greenspaces

The voluntary creation of lists of materials determined to be appropriate for children and provision, via a browser or an online service or server filters, of an environment that allows children to go to or receive only such materials.

a. How effective is this Technology/Method in preventing access by children to harmful to minor's material (on a scale of 0-10, with 0 being ineffective and 10 being completely effective)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (6)
Bastian (6)
Berman (8)
DeRosier (6)
Flores (2)
Ganier (7)
Hughes (7)
Parker (5)
Schmidt (2)
Schrader (9)
Shapiro (8)
Srinivasan (8)
Talbert (8)
Telage (7)
Vradenburg (9)

b. How accessible is this Technology/Method (easy to find, implement and use) (on a scale of 0-10, with 0 being totally inaccessible and 10 being totally accessible)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (6)
Bastian (5)
Berman (7)
DeRosier (6)
Flores (3)
Ganier (7)
Hughes (6)
Parker (6)
Schmidt (8)
Schrader (8)
Shapiro (7)
Srinivasan (9)
Talbert (7)
Telage (8)
Vradenburg (9)

c. How costly is this Technology/Method to users (considering direct and indirect costs) (on a scale of 0-10, with 0 being free and 10 being very expensive)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (NA)
Bastian (3)
Berman (3)
DeRosier (3)
Flores (3)
Ganier (4)
Hughes (1)
Parker (2)
Schmidt (1)
Schrader (2)
Shapiro (1)
Srinivasan (0)
Talbert (2)
Telage (3)
Vradenburg (1)

d. How costly is this Technology/Method to sources of otherwise lawful adult content that would be deemed harmful to minors under COPA (considering direct and indirect costs) (on a scale of 0-10, with 0 being free and 10 being very expensive)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (2)
Bastian (0)
Berman (4)
DeRosier (1)
Flores (2)
Ganier (2)
Hughes (0)
Parker (0)
Schmidt (5)
Schrader (0)
Shapiro (5)
Srinivasan (0)
Talbert (0)
Telage (1)
Vradenburg (0)

e. How extensive are the adverse impacts of this technology on privacy (on a scale of 0-10, with 0 meaning no adverse impacts and 10 meaning very substantial adverse impacts)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (1)
Bastian (4)
Berman (1)
DeRosier (2)
Flores (7)
Ganier (1)
Hughes (0)
Parker (0)
Schmidt (1)
Schrader (0)
Shapiro (1)
Srinivasan (0)
Talbert (0) (1)
Telage (1)
Vradenburg (0)

f. How extensive are the adverse impacts of this technology on first amendment values (protection of lawful adult speech) (on a scale of 0-10, with 0 meaning no adverse impacts and 10 meaning very substantial adverse impacts)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (5)
Bastian (5)
Berman (3)
DeRosier (5)
Flores (7)
Ganier (4)
Hughes (4)
Parker (0)
Schmidt (1)
Schrader (3)
Shapiro (1)
Srinivasan (0)
Talbert (3)
Telage (3)
Vradenburg (1)

g. How extensive are the adverse impacts of this technology on law enforcement (on a scale of 0-10, with 0 meaning no adverse impacts, and 10 meaning very substantial adverse impacts)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (0)
Bastian (0)
Berman (0)
DeRosier (0)
Flores (0)
Ganier (1)
Hughes (0)
Parker (0)
Schmidt (1)
Schrader (0)
Shapiro (0)
Srinivasan (0)
Talbert (0)
Telage (4) (1)
Vradenburg (0)

15. Monitoring and time-limiting tools

Use (typically at the PC) of software that creates logs showing details of a child's online activities and, optionally, enforces rules regarding the amount of time that may be spent online. Such systems may track both web use and email and instant messaging activities. In analyzing this technology/method, the Commission will assume that the child is told that the monitoring is taking place and that only the parent has access to the resulting information.

(Assumes use by parents in home. Separate discussions of schools and libraries).

a. How effective is this Technology/Method in preventing access by children to harmful to minor's material (on a scale of 0-10, with 0 being ineffective and 10 being completely effective)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (3)
Bastian (8)
Berman (6)
DeRosier (7)
Flores (6)
Ganier (4)
Hughes (4+)
Parker (6)
Schmidt (4)
Schrader (6)
Shapiro (6)
Srinivasan (8)
Talbert (5)
Telage (5)
Vradenburg (5)

b. How accessible is this Technology/Method (easy to find, implement and use) (on a scale of 0-10, with 0 being totally inaccessible and 10 being totally accessible)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (2)
Bastian (8)
Berman (5)
DeRosier (4)
Flores (8)
Ganier (3)
Hughes (7)
Parker (4)
Schmidt (7)
Schrader (7)
Shapiro (6)
Srinivasan (5)
Talbert (2)
Telage (4)
Vradenburg (5)

c. How costly is this Technology/Method to users (considering direct and indirect costs) (on a scale of 0-10, with 0 being free and 10 being very expensive)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (4)
Bastian (5)
Berman (3)
DeRosier (3)
Flores (8)
Ganier (8)
Hughes (5)
Parker (7)
Schmidt (2)
Schrader (3)
Shapiro (4)
Srinivasan (5)
Talbert (2)
Telage (4)
Vradenburg (1)

d. How costly is this Technology/Method to sources of otherwise lawful adult content that would be deemed harmful to minors under COPA (considering direct and indirect costs) (on a scale of 0-10, with 0 being free and 10 being very expensive)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (0)
Bastian (0)
Berman (0)
DeRosier (1)
Flores (0)
Ganier (1)
Hughes (0)
Parker (0)
Schmidt (1)
Schrader (0)
Shapiro (0)
Srinivasan (0)
Talbert (1)
Telage (0)
Vradenburg (0)

e. How extensive are the adverse impacts of this technology on privacy (on a scale of 0-10, with 0 meaning no adverse impacts and 10 meaning very substantial adverse impacts)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (7)
Bastian (0)
Berman (5)
DeRosier (1)
Flores (1)
Ganier (6)
Hughes (1)
Parker (3)
Schmidt (9)
Schrader (5)
Shapiro (4)
Srinivasan (0)
Talbert (0)
Telage (5)
Vradenburg (6)

f. How extensive are the adverse impacts of this technology on first amendment values (protection of lawful adult speech) (on a scale of 0-10, with 0 meaning no adverse impacts and 10 meaning very substantial adverse impacts)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (3)
Bastian (0)
Berman (5)
DeRosier (4)
Flores (0)
Ganier (5)
Hughes (1)
Parker (3)
Schmidt (8)
Schrader (5)
Shapiro (4)
Srinivasan (0)
Talbert (0)
Telage (5)
Vradenburg (3)

g. How extensive are the adverse impacts of this technology on law enforcement (on a scale of 0-10, with 0 meaning no adverse impacts, and 10 meaning very substantial adverse impacts)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (0)
Bastian (0)
Berman (0)
DeRosier (0)
Flores (0)
Ganier (0)
Hughes (0)
Parker (0)
Schmidt (1)
Schrader (0)
Shapiro (0)
Srinivasan (0)
Talbert (0)
Telage (1)
Vradenburg (0)

16. Acceptable use policies/family contracts

Establishment by a parent or an institution (school or library) of rules regarding the types of materials that may be accessed. Typically, such policies would be enforced by means of denial of further access in the event of a violation. Such policies may or may not be accompanied by monitoring that would allow the parent or institution to detect violations.

a. How effective is this Technology/Method in preventing access by children to harmful to minor's material (on a scale of 0-10, with 0 being ineffective and 10 being completely effective)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (2)
Bastian (2)
Berman (5)
DeRosier (6)
Flores (0)
Ganier (2)
Hughes (1)
Parker (3)
Schmidt (5)
Schrader (6)
Shapiro (8)
Srinivasan (9)
Talbert (4)
Telage (8)
Vradenburg (8)

b. How accessible is this Technology/Method (easy to find, implement and use) (on a scale of 0-10, with 0 being totally inaccessible and 10 being totally accessible)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (3)
Bastian (8)
Berman (8)
DeRosier (6)
Flores (6)
Ganier (7)
Hughes (7)
Parker (4)
Schmidt (8)
Schrader (6)
Shapiro (8)
Srinivasan (9)
Talbert (7)
Telage (4)
Vradenburg (5)

c. How costly is this Technology/Method to users (considering direct and indirect costs) (on a scale of 0-10, with 0 being free and 10 being very expensive)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (6)
Bastian (1)
Berman (0)

DeRosier (6)
Flores (9)
Ganier (1)
Hughes (2)
Parker (7)
Schmidt (1)
Schrader (0)
Shapiro (0)
Srinivasan (2)
Talbert (2)
Telage (6)
Vradenburg (1)

d. How costly is this Technology/Method to sources of otherwise lawful adult content that would be deemed harmful to minors under COPA (considering direct and indirect costs) (on a scale of 0-10, with 0 being free and 10 being very expensive)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (0)
Bastian (0)
Berman (0)
DeRosier (3)
Flores (0)
Ganier (2)
Hughes (0)
Parker (0)
Schmidt (1)
Schrader (0)
Shapiro (0)
Srinivasan (0)
Talbert (0)
Telage (0)
Vradenburg (0)

e. How extensive are the adverse impacts of this technology on privacy (on a scale of 0-10, with 0 meaning no adverse impacts and 10 meaning very substantial adverse impacts)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (6)
Bastian (0)
Berman (3)
DeRosier (5)
Flores (0)
Ganier (1)
Hughes (0)
Parker (2)
Schmidt (1)
Schrader (1)
Shapiro (1)
Srinivasan (0)
Talbert (0)
Telage (3)
Vradenburg (0)

f. How extensive are the adverse impacts of this technology on first amendment values (protection of lawful adult speech) (on a scale of 0-10, with 0 meaning no adverse impacts and 10 meaning very substantial adverse impacts)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (3)
Bastian (0)
Berman (2)
DeRosier (2)
Flores (0)
Ganier (1)
Hughes (0)
Parker (1)
Schmidt (1)
Schrader (0)
Shapiro (0)
Srinivasan (0)
Talbert (0)
Telage (2)
Vradenburg (0)

g. How extensive are the adverse impacts of this technology on law enforcement (on a scale of 0-10, with 0 meaning no adverse impacts, and 10 meaning very substantial adverse impacts)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (1)
Bastian (0)
Berman (0)
DeRosier (0)
Flores (2)
Ganier (1)
Hughes (0)
Parker (0)
Schmidt (1)
Schrader (0)
Shapiro (0)
Srinivasan (0)
Talbert (0)
Telage (1)
Vradenburg (0)

17. Increased prosecution

Governmental expenditure (at federal, state, and local levels) of more funds to investigate and prosecute online activities that are unlawful. While this "method" assumes a change in current governmental activity, the Commission will analyze its likely effectiveness (and potential adverse impacts) to provide a basis for its recommendations. The Commission will assume that US law could not practically be enforced against all content sources located in other countries with differing legal standards for content. The Commission will assume that the additional resources would not be used to prosecute lawful adult speech.

a. How effective is this Technology/Method in preventing access by children to harmful to minor's material (on a scale of 0-10, with 0 being ineffective and 10 being completely effective)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (8)
Bastian (8)
Berman (3)
DeRosier (9)
Flores (8)
Ganier (8)
Hughes (9)
Parker (10)
Schmidt (6)
Schrader (2)
Shapiro (5)
Srinivasan (3)
Talbert (9)
Telage (3) (5)
Vradenburg (5)

b. How accessible is this Technology/Method (easy to find, implement and use) (on a scale of 0-10, with 0 being totally inaccessible and 10 being totally accessible)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (5)
Bastian (5)
Berman (5)
DeRosier (8)
Flores (9)
Ganier (8)
Hughes (8)
Parker (8)
Schmidt (4)
Schrader (6)
Shapiro (7)
Srinivasan (10)
Talbert (7)
Telage (4)
Vradenburg (1)

c. How costly is this Technology/Method to users (considering direct and indirect costs) (on a scale of 0-10, with 0 being free and 10 being very expensive)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (0)
Bastian (0)
Berman (4)
DeRosier (2)
Flores (0)
Ganier (1)
Hughes (0)
Parker (0)
Schmidt (6)
Schrader (1)
Shapiro (1)
Srinivasan (0)
Talbert (0)
Telage (3)
Vradenburg (0)

d. How costly is this Technology/Method to sources of otherwise lawful adult content that would be deemed harmful to minors under COPA (considering direct and indirect costs) (on a scale of 0-10, with 0 being free and 10 being very expensive)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (6)
Bastian (6)
Berman (6)
DeRosier (2)
Flores (0)
Ganier (3)
Hughes (2)
Parker (0)
Schmidt (2)
Schrader (8)
Shapiro (7)
Srinivasan (3)
Talbert (0)
Telage (10)
Vradenburg (5)

e. How extensive are the adverse impacts of this technology on privacy (on a scale of 0-10, with 0 meaning no adverse impacts and 10 meaning very substantial adverse impacts)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (5)
Bastian (2)
Berman (5)
DeRosier (2)
Flores (2)
Ganier (5)
Hughes (0)
Parker (0)
Schmidt (1)
Schrader (7)
Shapiro (3)
Srinivasan (1)
Talbert (0)
Telage (5)
Vradenburg (0)

f. How extensive are the adverse impacts of this technology on first amendment values (protection of lawful adult speech) (on a scale of 0-10, with 0 meaning no adverse impacts and 10 meaning very substantial adverse impacts)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (3)
Bastian (2)
Berman (5)
DeRosier (2)
Flores (0)
Ganier (5)
Hughes (0)
Parker (0)
Schmidt (2)
Schrader (5)
Shapiro (3)
Srinivasan (2)
Talbert (0)
Telage (5)
Vradenburg (4)

g. How extensive are the adverse impacts of this technology on law enforcement (on a scale of 0-10, with 0 meaning no adverse impacts, and 10 meaning very substantial adverse impacts)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (0)
Bastian (0)
Berman (0)
DeRosier (0)
Flores (0)
Ganier (0)
Hughes (0)
Parker (0)
Schmidt (0)
Schrader (0)
Shapiro (0)
Srinivasan (0)
Talbert (0)
Telage (10) (0)
Vradenburg (0)

18. Real time Content Monitoring/Blocking

Use of real time monitoring methods to detect and block HTM material sent via email, instant messaging, chat rooms and Usenet in addition to the web. Such monitoring assumes the ability to detect HTM materials in areas where filtering may apply.

a. How effective is this Technology/Method in preventing access by children to harmful to minor's material (on a scale of 0-10, with 0 being ineffective and 10 being completely effective)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (NA)
Bastian (9)
Berman (4)

DeRosier (NA)
Flores (6)
Ganier (6)
Hughes (7) (10)
Parker (7)
Schmidt (NA)
Schrader (NA)
Shapiro (4)
Srinivasan (2)
Talbert (6)
Telage (4)
Vradenburg (NA)

b. How accessible is this Technology/Method (easy to find, implement and use) (on a scale of 0-10, with 0 being totally inaccessible and 10 being totally accessible)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (NA)
Bastian (5)
Berman (5)
DeRosier (NA)
Flores (4)
Ganier (5)
Hughes (4)
Parker (5)
Schmidt (NA)
Schrader (NA)
Shapiro (5)
Srinivasan (4)
Talbert (2)
Telage (5)
Vradenburg (NA)

c. How costly is this Technology/Method to users (considering direct and indirect costs) (on a scale of 0-10, with 0 being free and 10 being very expensive)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (NA)
Bastian (2)
Berman (4)
DeRosier (NA)
Flores (5)
Ganier (6)
Hughes (2)
Parker (5)
Schmidt (NA)
Schrader (NA)
Shapiro (4)
Srinivasan (2)
Talbert (2)
Telage (4)
Vradenburg (NA)

d. How costly is this Technology/Method to sources of otherwise lawful adult content that would be deemed harmful to minors under COPA (considering direct and indirect costs) (on a scale of 0-10, with 0 being free and 10 being very expensive)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (NA)
Bastian (0)
Berman (2)
DeRosier (NA)
Flores (8)
Ganier (1)
Hughes (0)
Parker (0)
Schmidt (NA)
Schrader (NA)
Shapiro (10)
Srinivasan (10)
Talbert (0)
Telage (0)
Vradenburg (NA)

e. How extensive are the adverse impacts of this technology on privacy (on a scale of 0-10, with 0 meaning no adverse impacts and 10 meaning very substantial adverse impacts)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (NA)
Bastian (0)
Berman (7)
DeRosier (NA)
Flores (2)
Ganier (6)
Hughes (0)
Parker (2)
Schmidt (4)
Schrader (NA)
Shapiro (6)
Srinivasan (4)
Talbert (0)
Telage (6)
Vradenburg (NA)

f. How extensive are the adverse impacts of this technology on first amendment values (protection of lawful adult speech) (on a scale of 0-10, with 0 meaning no adverse impacts and 10 meaning very substantial adverse impacts)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (NA)
Bastian (1)
Berman (6)
DeRosier (NA)
Flores (2)
Ganier (5)
Hughes (1)
Parker (3) (2)
Schmidt (4)
Schrader (NA)
Shapiro (3)
Srinivasan (NA)
Talbert (1)

Telage (6)
Vradenburg (NA)

g. How extensive are the adverse impacts of this technology on law enforcement (on a scale of 0-10, with 0 meaning no adverse impacts, and 10 meaning very substantial adverse impacts)?

0 1 2 3 4 5 6 7 8 9 10

Balkam (NA)
Bastian (0)
Berman (1)
DeRosier (NA)
Flores (0)
Ganier (0)
Hughes (0)
Parker (0)
Schmidt (NA)
Schrader (NA)
Shapiro (0)
Srinivasan (0)
Talbert (0)
Telage (2)
Vradenburg (NA)

COPA Commission

Information and Resources About the Commission on Online Child Protection (COPA)

Hosted by the Congressional Internet Caucus Advisory Committee

Appendix G, Catalog of Drawer Files

Label Name or Folder Label in Bold.

COPA April 28 Meeting

Briefing Folder

COPA Hearing #1, Additional Testimony

GetNetwise Press Clips, prepared for the COPA Commission. Binder with 8 sections, approximately 200 pages. www.getnetwise.org.

COPA Hearing #1, Transcripts

7 VHS Tapes, COPA Commission 6/8-9/2000, Room 432, Federal Trade Commission, Washington, DC.

Transcripts, COPA Commission 6/8-9/2000. Prepared by ARTI Transcripts, www.artitranscripts.com. Washington, DC.

> 2 Volumes:
> "Common Resources for Parents and One-Click-Away Resources." 207p.
> "Age Verification Technologies." 116p.

COPA Hearing #2 Additional Testimony

Materials from Entertainment Software Rating Board

> Letter from Arthur Pober
> Folder with background information on ESRB and ESRBi

Materials from Virginia Beach Public Library. All materials give reference to website http://www.virginiabeach.va.us/dept/library

> "Internet Help Sheet"
> "Kids & Parents, Using the Library Together" - yellow 3-fold sheet
> "Can I Trust This Resource" - green 12" bookmark
> Printouts:
> "Public Access Welcome Page with Internet Use Policy Summary"
> http://intranet.vbpl.city.virginia-beach.va.us/ba/ 07/19/00
> "Parents FAQ's" http://intranet.vbpl.virginia0beach.va.us/kidsnet/knfaq.html 07/20/00

COPA Hearing #2, Transcripts

6 VHS Tapes, COPA Commission 7/20-21/2000, Jepson Alumni Center, University of Richmond, VA. Prepared by VAVS Productions, (804)935-3933.

Transcripts, COPA Commission 7/20-21/2000. Prepared by ARTI Transcripts, www.artitranscripts.com. Washington, DC.

3 Volumes:
"Filtering, Labeling and Rating Technologies, 7/20." 154p.
"Afternoon Session." 155-316p.
"Filtering, Labeling and Rating Technologies, 7/21." 174p.

COPA Hearing #3 Additional Testimony

Berman, Jerry and Daniel J. Weitzner. "Abundance and User Control: Renewing the Democratic Heart of the First Amendment in the Age of Interactive Media." The Yale Law Journal. V. 104, N. 7. May 1995, p.1619-1637.

Briefing Book on User Empowerment and Free Speech Online. Questions about the group can be addressed to the Center for Democracy and Technology, at webmaster@cdt.org.

Willard, Nancy. "Legal and Ethical Issues Related to the Use of the Internet in K-12 Schools." Brigham Young University Education and Law Journal. V. 2000, N.2, p.225-286.

Materials Submitted by Robin Raskin: (2 copies available)

Photocopy of *FamilyPC* Magazine, March 2000, select pages;
Cover, p.79-88, 90-96.
Articles: Jabs, Carolyn. "Sex, Lies, and Children: What Parents Don't Know About the Internet." p. 79-88.
Lewis, Anne. "There Oughta Be a Law." p. 91-93.
Dumas, Lynne. S. "The World Wide Worry." p. 94,96.
Summary and Select Results of FamilyPC 2000 survey, compiled by Digital Research, Inc.

Internet Industry Association, "Internet Industry Codes of Practice, Codes for Industry Self Regulation in Areas of Internet Content Pursuant to the Requirements of the Broadcasting Services Act 1992 As Amended." December 1999. http://www.iia.net.au/

Materials submitted by Jean Armour Polly

Polly, Jean Armour. Internet Yellow Pages(+ book)

Materials submitted by William L. Tafoya:

Lee, Wayne. "Child Pornography." Frankfort Police Department. August, 2000.

Written Statement of Kevin Manson, Webmaster, Cybercop Secure

Communities, prepared for the Congressional Hearings before the Committee on Science, Subcommittee on Technology and Subcommittee on Basic Research of the House of Representatives on: "Cyberporn: Protecting our Children from the Back Alleys of the Internet." July 26, 1995.

Materials submitted by Marcel Machill:

Machill, Marcel and Waltermann, J., eds. Protecting Our Children on the Internet. Towards a New Culture of Responsibility. Gutersloh: Bertelsmann Foundation Publishers 2000.

COPA Report

U.S. House of Representatives, 105th Congress, 2d Session. Child Online Protection Act, Report 105-775, 32pp.

COPA 3rd Circuit Appeal

American Civil Liberties Union, et al., Plaintiffs-Appellees, v. Janet Reno, in her official capacity as Attorney General of the United States, Defendant-Appellant. No. 99-1324

Department of Commerce

Letter to the Commission from Gregory L. Rohde, Assistant Secretary for Communications and Information. June 8,2000, 3pp. Re: creation of a new gTLD. (7 copies)

National Law Center for Children and Families

3-fold Pamphlet on National Law Center for Children and Families.

Correspondence to Hons. Bliley, Tauzin, & Oxley. Re: Supplement to the Record of Hearing on H.R. 3783, submitted by Bruce Taylor and Chadwicke Groover. September 22, 1998. 9pp.

Enough is Enough

Child Online Protection Act, Briefing Notes. *Enough is Enough*. Santa Ana, CA. 24p, bound. (2copies)

Watson, Bruce and Shyla Rae Welch. "Just Harmless Fun? Understanding the Impact of Pornography." Enough is Enough. Santa Ana, CA. www.enough.org. 15p. (2 copies)

Family Click

Background folders on FamilyClick (5 copies)

"FamilyClick Connecting Families"
"FamilyClick Fact Sheet"
FamilyClick launch announcement
FamilyClick Executives List

Hughes, Donna Rice. "The Positives and Perils of the Internet: Working Together to Make Your Family's Online Experience Safe and Fun." December, 1, 1999.

Filters and Freedom

Filters & Freedom, Free Speech Perspectives on Internet Content Controls. *Electronic Privacy Information Center*, Washington, DC © 1999. 174p.

National Center for Missing and Exploited Children

"Online Victimization: A Report on the Nation's Youth." Prepared by the Crimes Against Children Research Center. Finkelhor, Mitchell, Wolak, eds. June 2000. 50p. (7 copies)

Net Nanny

Independent Endorsements of Net Nanny.
Reprints of Press Articles evaluating Net Nanny. (12p)
Printouts of various web sites/indexes pertaining to k-12 education resources.

Virginia Beach Public Library

(additional copies, all material listed in "Testimony Hearing 2" Folder)
All materials give reference to website http://www.virginia-beach.va.us/dept/library for further information.
"Internet Help Sheet" (10 copies)
"Kids & Parents, Using the Library Together" - yellow 3-fold sheet (9 copies)
"Can I Trust This Resource" - green 12" bookmark (12 copies)

Pacel

Folders containing information describing ChildWatch Filter, a product of Pacel Corporation. (4 copies)

CD-Rom, ChildWatch Software.
ChildWatch Sponsorship Information.
Pacel Corporate Overview

BO Dietl Computer Corp

CD-Rom Software, Bo Dietl's One Tough Computer Cop. Computer Concepts Corporation. Bohemia, NY.

Technology Matrix Submissions

The Following is a list of hard-copy matrix submissions available.

Ken Baker of FamilyClick has compiled these and will have available electronically via CD-Rom Appendix E.

"Cyber Patrol" : Cyber Patrol, 1900 West Park Drive, Suite 180, Westbourough, MA 01581.

"Anti-Defamation League Hate Filter": Anti-Defamation League, 823 United Nations Plaze, New York, NY 10017.

"X-Stop" : Log-On Data Corp., 828 West Taft Avenue, Orange, CA 92865-4232.

"N2H2 For Schools (AKA Bess Filtering)," "N2H2 For Libraries," "N2H2 For Business" : N2H2, 900 Fourth Avenue, Suite 3400, Seattle, WA 98164.

"ChildWatch" : Pacel Corp. 8870 Rixiew Lane, Suite 201, Manassas, VA 20109. Note: Matrix submission is inside a Pacel Corporation folder including software.

"PlanetGood" : PlanetGood Technologies, Inc. (formerly BrowsSafe.com), 7202 E. 87th St. Suite 109, Indianapolis, IN 46256.

"CharacterLink" : CharacterLink, 2820 N. Meridian Street, Indianapolis, IN 46208.

"RSACi": ICRA, 3460 Olney-Laytonsville Road, Suite 202, Olney, MD 20832.

"Cyber Snoop" : Pearl Software, Inc., 64 E. Uwchian Ave., Suite 230, Exton, PA 19341.

"Yahooligans!" : Yahoo!, 3420 Central Expressway, Santa Clara, CA 95051.

"Desktop Surveillance" : Tech Assist, Inc., 18830 U.S. 19 North, Suite 323, Clearwater, FL 33764.

"ZeekSafe" : Zeeks.com, Inc., 5200 SW Macadam Ave., Portland, OR 97201.

"FamilyClick" : FamilyClick.com, LLC, 2877 Guardian Lane, Suite 300, Virginia Beach, VA 23452.

"WinGuardian" : WinGuardian, P.O. Box 3531, Boulder, CO 80307.

"Awesome Library" : Evaluation and Development Institute (EDI), 100 Kerr Pkwy., No. 39, Lake Oswego, OR 97035.

"SafeSurf" : SafeSurf, 16032 Sherman Way, Suite 58, Van Nuys, CA 91406.

"Integrity Online" : Integrity Online, 5800 One Parkins Place, Suite 9A, Baton Rouge, LA 70808.

"Safexplorer" : Safexplorer, 700-509 Richards St., Vancouver, BC, Canada V652Z6.

"NetNanny" : NetNanny Software, Inc., 15831 NE 8th, Suite 200, Bellevue, WA 98008.

"E-Junk" : Obvious Solutions, 500 Summer St., Suite 404, Stamford, CT 06901.

"Integrity Online" : Integrity Online of Wichita Falls, TX, 3515 McNiel, Wichita Falls, TX 76308.

"Cyber Sentinel V2.0" : Security Software Systems, 1998 Bucktail Lane, Sugar Grove, IL 60554

"WIPE" : TM Stanford University, Computer Science Dept., Stanford University, 94305.

"Internet Safari" ; Heartsoft, Inc., 3101 N. Hemlock Circle, Broken Arrow, OK 74014.

"iForAll" ; InForAll, Inc., 12200 Tech Rd. #303, Silver Spring, MD 20904.

"iWayPatrol, GBTW2000, children's dept., ispFamilyFilter, safEmail" ; iTECH, Inc., 6601 Washington Avenue, Racine, WI 53406.

"Safe Access" ; Safe Access, P.O. Box 2757, Flagstaff, AZ 86003.

"Dotsafe" ; Dotsafe, Inc., 8181 South 48th Street #120, Phoenix, AZ 85044.

"S4F Technologies" ; Family Connect, 2448 E. 81st Street, Suite 3300, Tulsa, OK 74137.

"Digimarc" ; Digimarc Corp., 19801 SW 72nd Ave., Ste. 250, Tualatin, OR 97062.

"Realtime Sentry" ; eplace2go, inc., 1117 South 22nd St., Birmingham, AL 35205.

"BASCOM" ; BASCOM Global Internet Services, Inc., 275 Marcus Boulevard, Suite R, Hauppauge, NY 11788

Correspondence to the Commission

5/25 4p. facsimile to the commission from Commissioner DeRosier.

- 5/25 Memo To: R. Hurlocker, From: A. DeRosier, Subject: COPA.
- 5/24 Memo To: A. DeRosier, From: R. Hurlocker, Subject: COPA.

5/26 3p. facsimile to the commission from Commissioner DeRosier.

- 5/26 Memo To: R. Hurclocker, From: A. DeRosier, Subject: Your Advice.
- 5/25 Email To: A. DeRosier, From: R. Hurlocker, Subject: COPA.

[Home] [Final Report] [About this Site] [FAQ] [The Commission] [Press Room]
[Meetings and Hearings] [Research Papers] [Privacy Policy]

webmaster@copacommission.org / Copyright © 2000

VI. CONCLUSION

The Commission appreciates the opportunity to have served the Congress of the United States by studying technologies and methods designed to reduce access by minors to "harmful to minors" material on the Internet. We respectfully submit this document as our final Report.

Previous: Proposed Future Work Next: Appendix

[Home] [Final Report] [About this Site] [FAQ] [The Commission] [Press Room]
[Meetings and Hearings] [Research Papers] [Privacy Policy]

webmaster@copacommission.org / Copyright © 2000

BEST COPY AVAILABLE

V. PROPOSED FUTURE WORK

The Commission is concerned that its lack of funding and short timetable has limited the inquiry in which it has been able to engage. We anticipate that, with additional resources and an extension of the statutorily allotted time for submission of this report, the Commission would have undertaken the following efforts to provide the Congress with a more in-depth and detailed report:

1. **Engage in a more robust analysis of technologies and methods.**
    - Conduct a more in-depth examination of individual technologies. This examination could include convening additional hearings on technologies about which we received insufficient testimony and observing technology demonstrations.
    - Present our recommendations for review by a panel of technical experts.
    - Investigate new technologies that came to the Commission's attention.
    - Clarify and break out the criteria and assumptions for evaluation of technologies and methods to allow the Commission to make more meaningful and specific assessments of individual technologies. Such an approach would allow the Commission to examine the distinct Constitutional and privacy impact, as well as the usefulness of these technologies in the home, school and libraries.
2. **Investigate the criteria and explore models for an independent testing lab that would provide consistent, reliable evaluation of technologies and provide an optimal service to the industry and consumers.**
3. **Solicit input from additional operators of filtering and monitoring systems.**

While this additional effort would have been desirable, it does not detract from the fact that the information gathered by the Commission was significant in quality and quantity, and provides an ample basis for our conclusions and recommendations.

Previous: Affirmative Defenses Next: Conclusion

BEST COPY AVAILABLE

[Home] [Final Report] [About this Site] [FAQ] [The Commission] [Press Room]
[Meetings and Hearings] [Research Papers] [Privacy Policy]

webmaster@copacommission.org / Copyright © 2000

COPA Commission

Information and Resources About the
Commission on Online Child Protection (COPA)
Hosted by the Congressional Internet Caucus Advisory Committee

IV. AFFIRMATIVE DEFENSES

The Congressional charge to the Commission states that "[t]he Commission shall conduct a study to identify technological or other methods that (A) will help reduce access by minors to material that is harmful to minors on the Internet; and (B) may meet the requirements for use as affirmative defenses for purposes of section 231(c)." Section 231(c), in turn, describes these requirements in terms of actions taken to restrict access by minors to material that is harmful to minors by means of "any reasonable measures that are feasible under available technology." Section 231(a) and (b) already recognize use of credit card and other age verification systems as affirmative defenses.

The Commission discussed whether and how to respond to the Congressional charge in Section B quoted above, in light of the fact that the COPA statute has now been preliminarily enjoined as unconstitutional. The Commission agreed that the question presented to it is not whether or not a particular technology or method should or should not be considered an affirmative defense, much less whether any statute should be found constitutional or unconstitutional. We interpret the question presented to the Commission in Section B as asking whether there are any feasible technologies or methods that are currently available and that may constitute "reasonable measures" to restrict access by minors to harmful to minors materials.

The Commission studied many different technologies and methods that may be used to restrict access by minors to harmful to minors materials. Some technologies did not meet all the statutory requirements because they are not feasible or are not currently available. We determined, however, that some of the technologies we analyzed, for example first party labeling, may become "reasonable" means of preventing child access to harmful to minors material when such technologies become more widely adopted in the marketplace. We did not have the time or resources, however, to conduct a detailed inquiry into the "reasonableness" of the use of any particular technology in the hypothetical context of an assertion of an affirmative defense under COPA. Because of the limitations on its study, the Commission did not conclude that any particular technology "may meet the requirements for use as affirmative defenses for purposes of section 231(c)."

Previous: Recommendations Next: Proposed Future Work

BEST COPY AVAILABLE

[Home] [Final Report] [About this Site] [FAQ] [The Commission] [Press Room]

webmaster@copacommission.org / Copyright © 2000